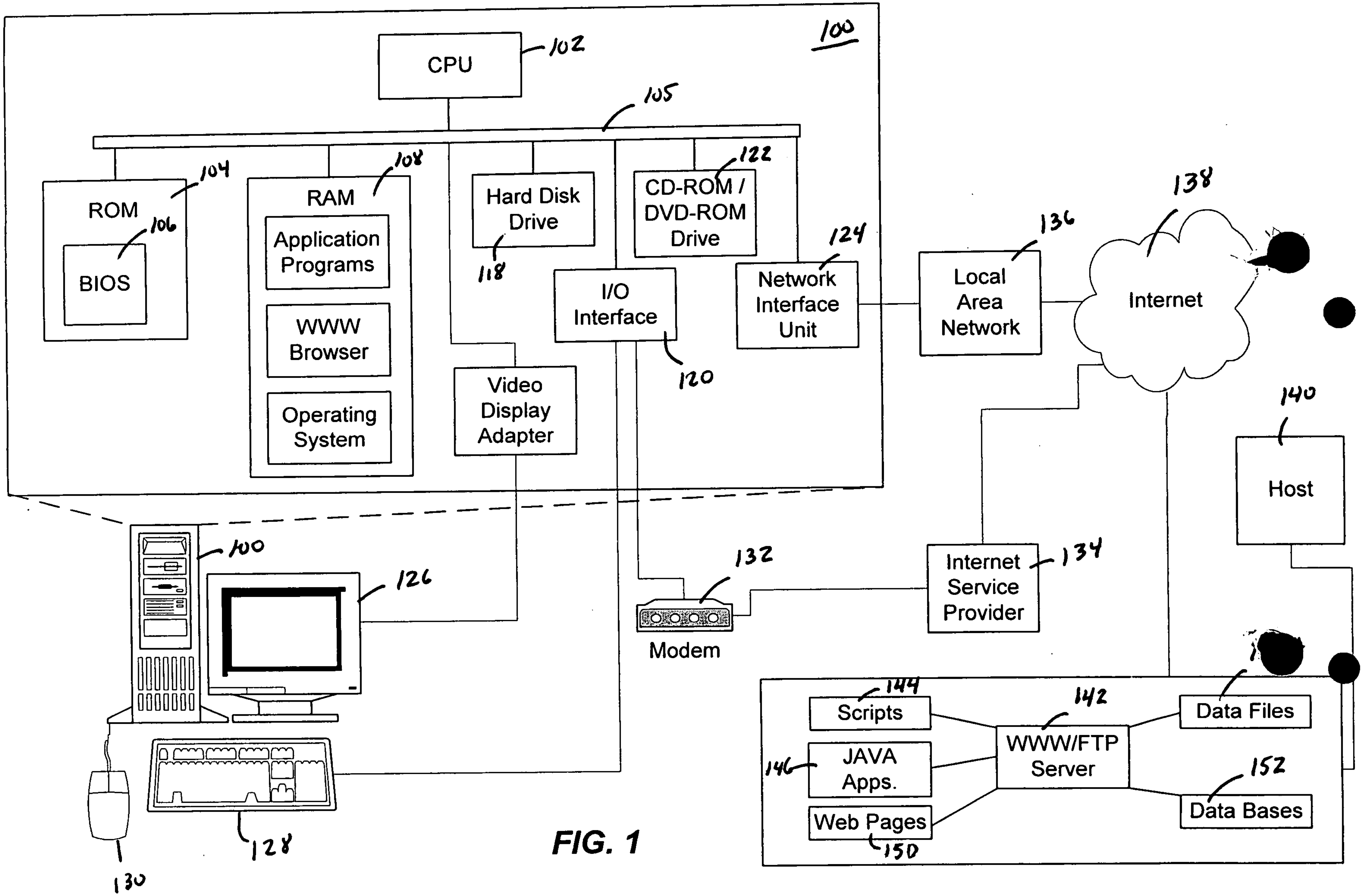

100
CPU
102
105
ROM
104
106
BIOS
RAM
108
Application Programs
WWW Browser
Operating System
Hard Disk Drive
118
CD-ROM / DVD-ROM Drive
122
I/O Interface
120
Network Interface Unit
124
Video Display Adapter
Local Area Network
136
Internet
138
Host
140
100
126
132
Modem
Internet Service Provider
134
128
130
Scripts
144
JAVA Apps.
146
Web Pages
150
WWW/FTP Server
142
Data Files
Data Bases
152

FIG. 1

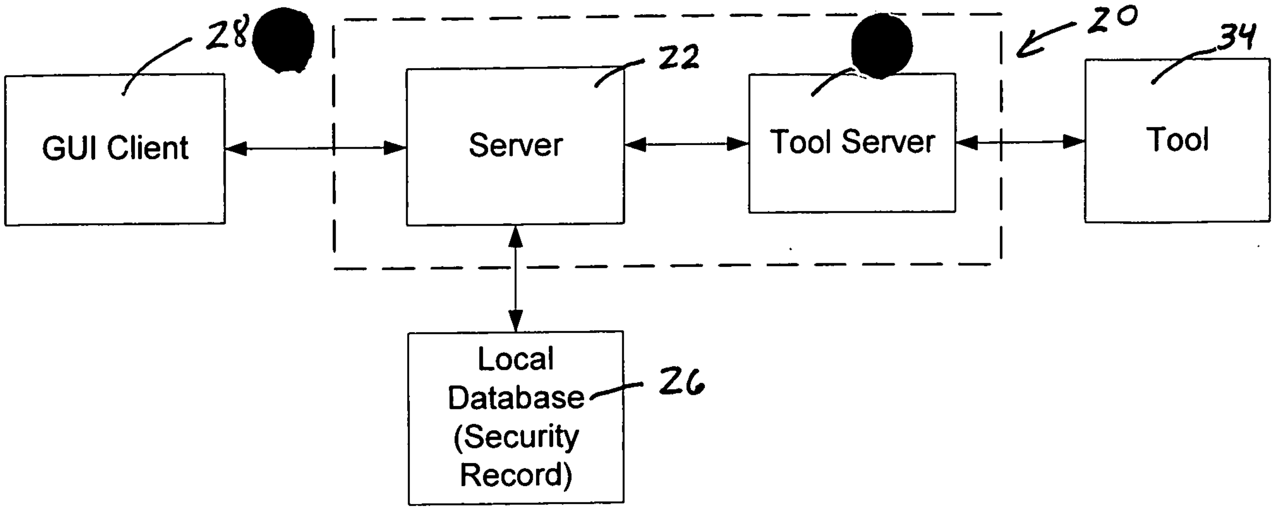

28
GUI Client
22
Server
Tool Server
20
34
Tool
Local Database (Security Record)
26

FIG. 2

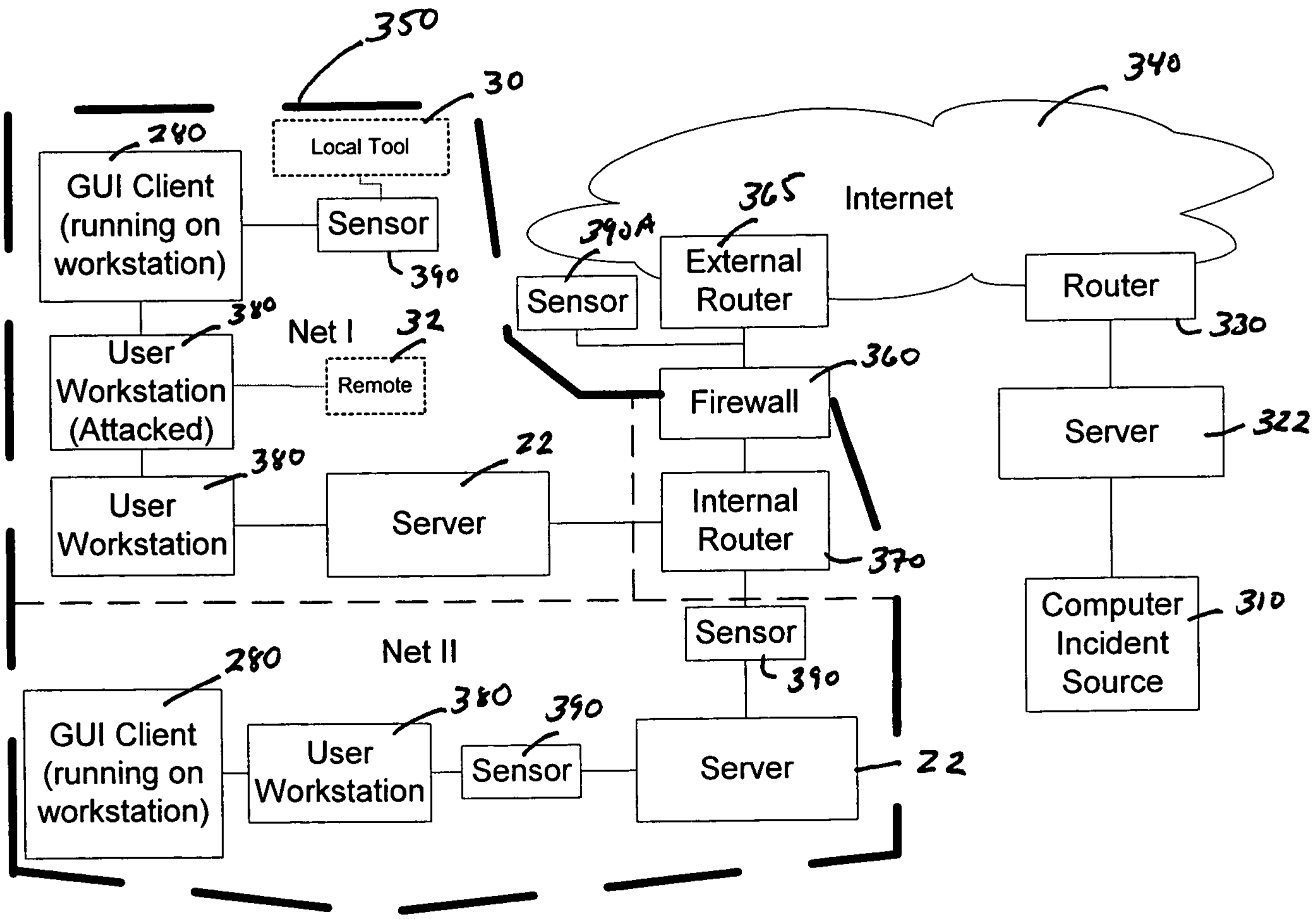
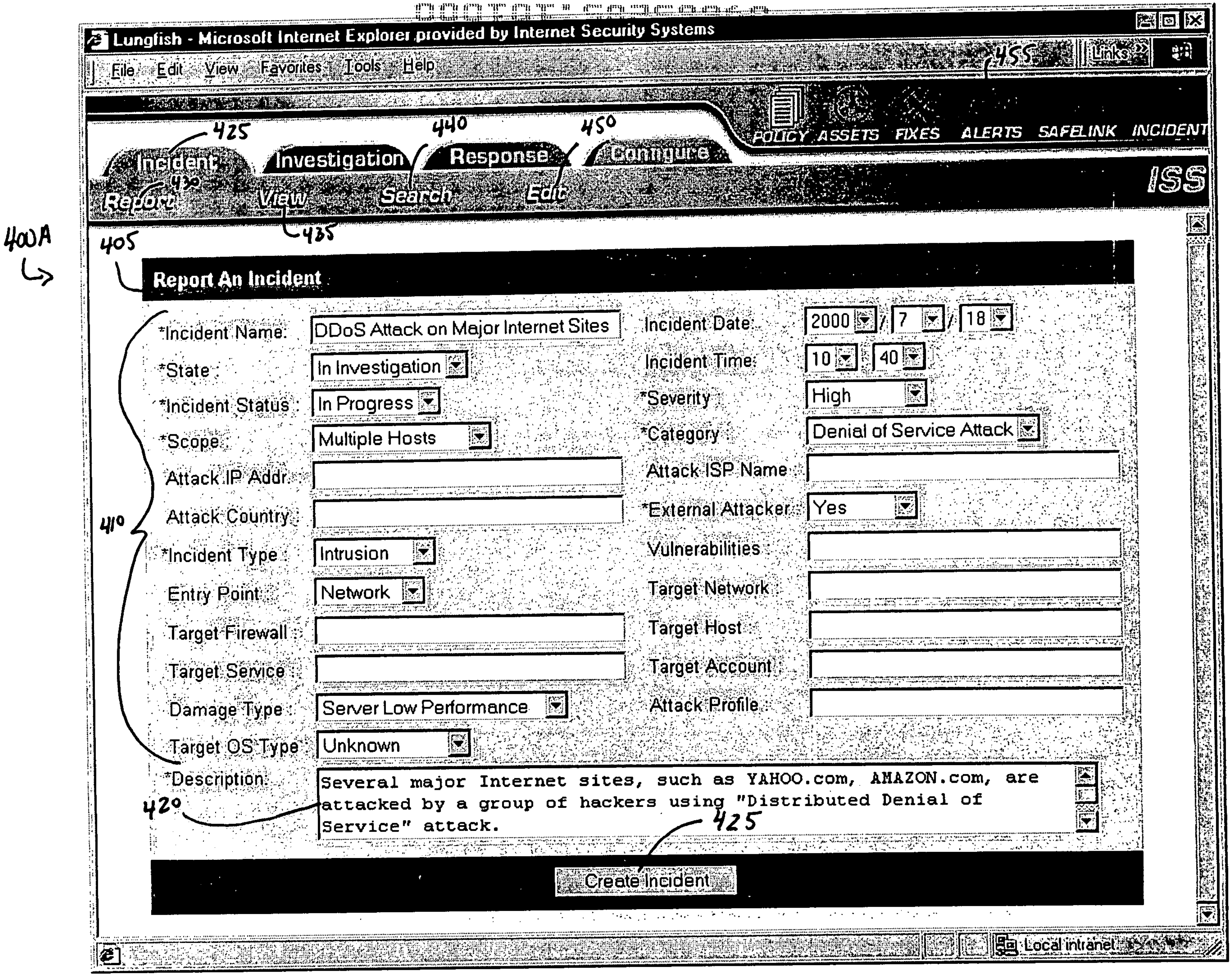

350
30
Local Tool
340
Internet
280
GUI Client (running on workstation)
Sensor
390
365
390A
Sensor
External Router
Router
330
380
User Workstation (Attacked)
Net I
32
Remote
360
Firewall
Server
322
380
User Workstation
22
Server
Internal Router
370
Computer Incident Source
310
Sensor
390
Net II
280
GUI Client (running on workstation)
380
User Workstation
390
Sensor
Server
22

FIG. 3



400A
Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
455
POLICY ASSETS FIXES ALERTS SAFELINK INCIDENT
ISS
425
Incident
Investigation
440
Response
450
Configure
430
Report
View
435
Search
Edit
405
410
420
425
Create Incident
Local intranet

Report An Incident

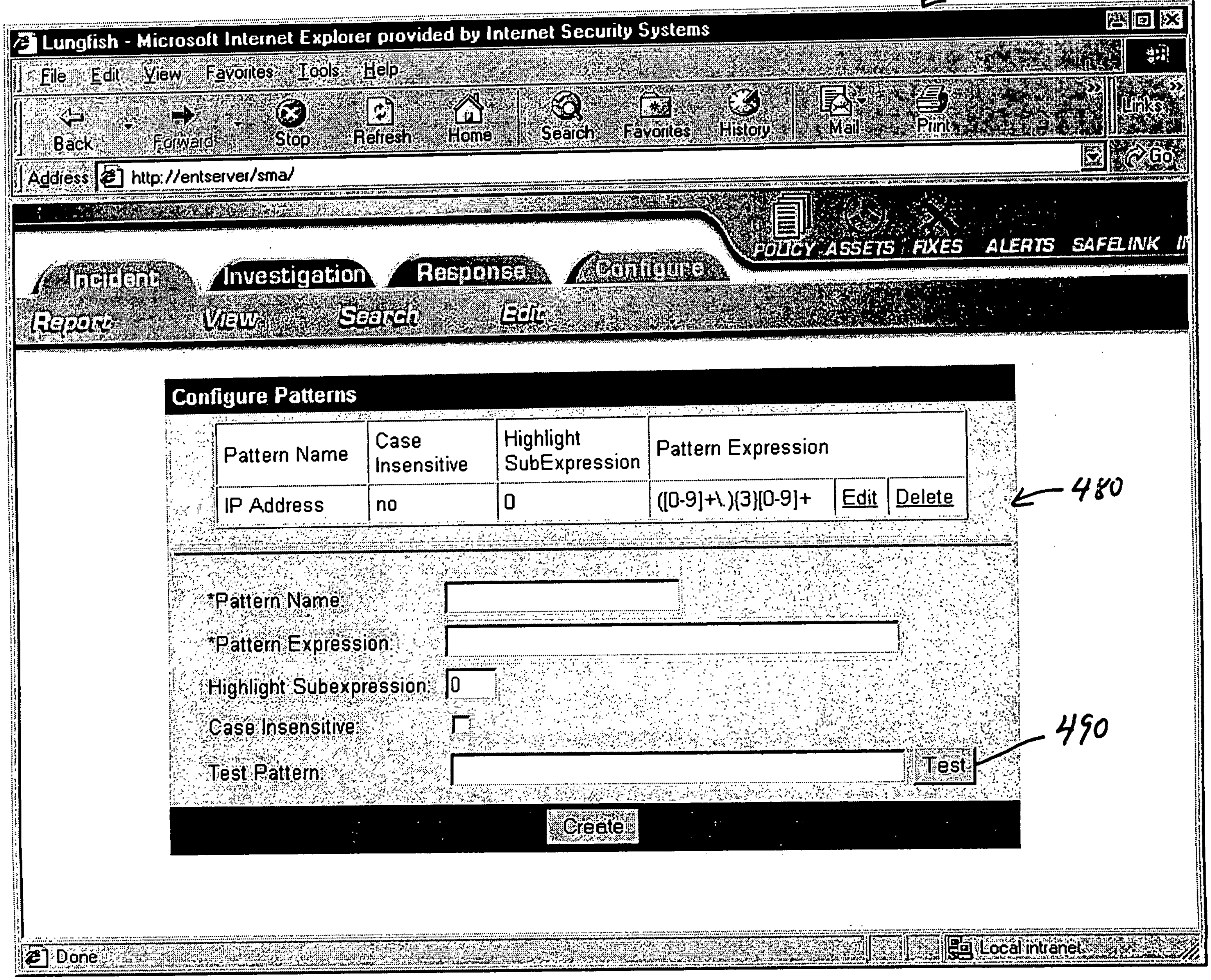
*Incident Name:	DDoS Attack on Major Internet Sites	Incident Date:	2000 / 7 / 18
*State :	In Investigation	Incident Time:	10 40
*Incident Status :	In Progress	*Severity	High
*Scope :	Multiple Hosts	*Category :	Denial of Service Attack
Attack IP Addr.		Attack ISP Name	
Attack Country :		*External Attacker :	Yes
*Incident Type :	Intrusion	Vulnerabilities :	
Entry Point :	Network	Target Network	
Target Firewall :		Target Host :	
Target Service :		Target Account :	
Damage Type :	Server Low Performance	Attack Profile :	
Target OS Type :	Unknown		

*Description:

```
Several major Internet sites, such as YAHOO.com, AMAZON.com, are
attacked by a group of hackers using "Distributed Denial of
Service" attack.
```

Fig. 4A

400B



Configure Patterns

Pattern Name	Case Insensitive	Highlight SubExpression	Pattern Expression		
IP Address	no	0	([0-9]+\.){3}[0-9]+	Edit	Delete

*Pattern Name:

*Pattern Expression:

Highlight Subexpression: 0

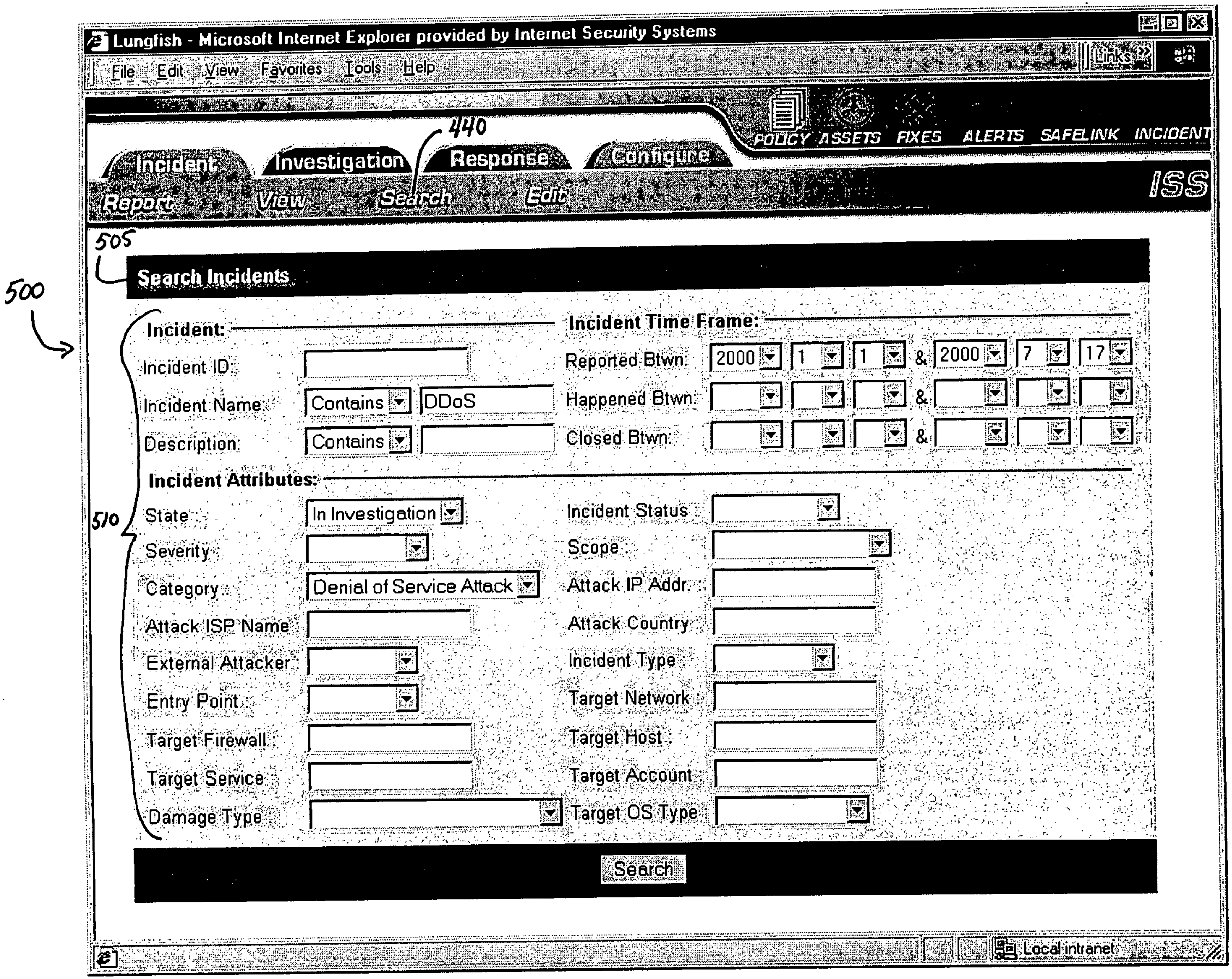
Case Insensitive: □

Test Pattern:

Test

Create

Fig. 4B



Lungfish - Microsoft Internet Explorer provided by Internet Security Systems

File Edit View Favorites Tools Help

Links »

POLICY ASSETS FIXES ALERTS SAFELINK INCIDENT

Incident Investigation Response Configure

Report View Search Edit

ISS

Search Incidents

Incident:

Incident ID:	
Incident Name:	Contains ▾ DDoS
Description:	Contains ▾

Incident Time Frame:

Reported Btwn:	2000 ▾	1 ▾	1 ▾	&	2000 ▾	7 ▾	17 ▾
Happened Btwn:	▾	▾	▾	&	▾	▾	▾
Closed Btwn:	▾	▾	▾	&	▾	▾	▾

Incident Attributes:

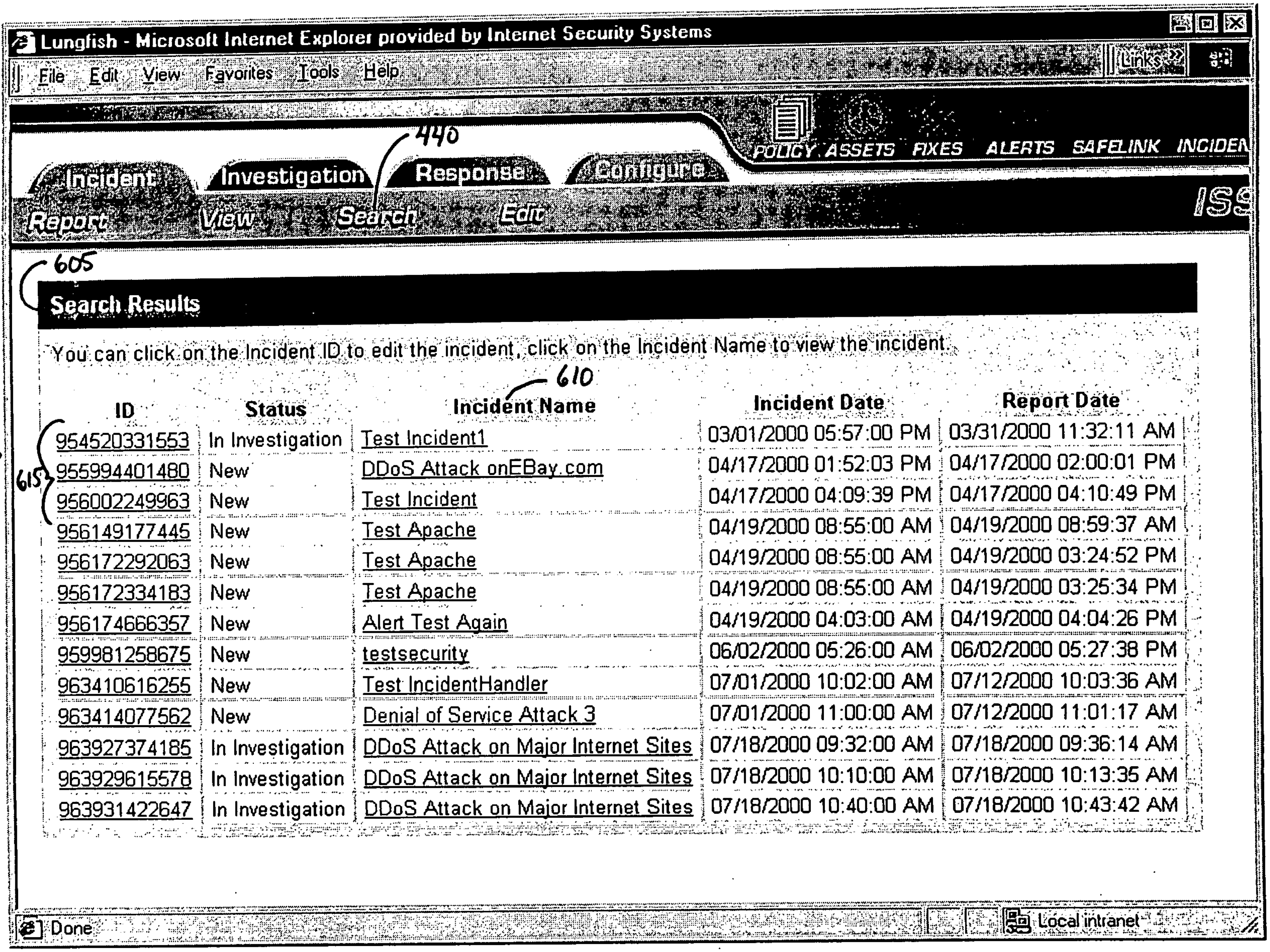
State:	In Investigation ▾	Incident Status:	▾
Severity:	▾	Scope:	▾
Category:	Denial of Service Attack ▾	Attack IP Addr.:	
Attack ISP Name:		Attack Country:	
External Attacker:	▾	Incident Type:	▾
Entry Point:	▾	Target Network:	
Target Firewall:		Target Host:	
Target Service:		Target Account:	
Damage Type:	▾	Target OS Type:	▾

Search

Local intranet

Fig. 5

600

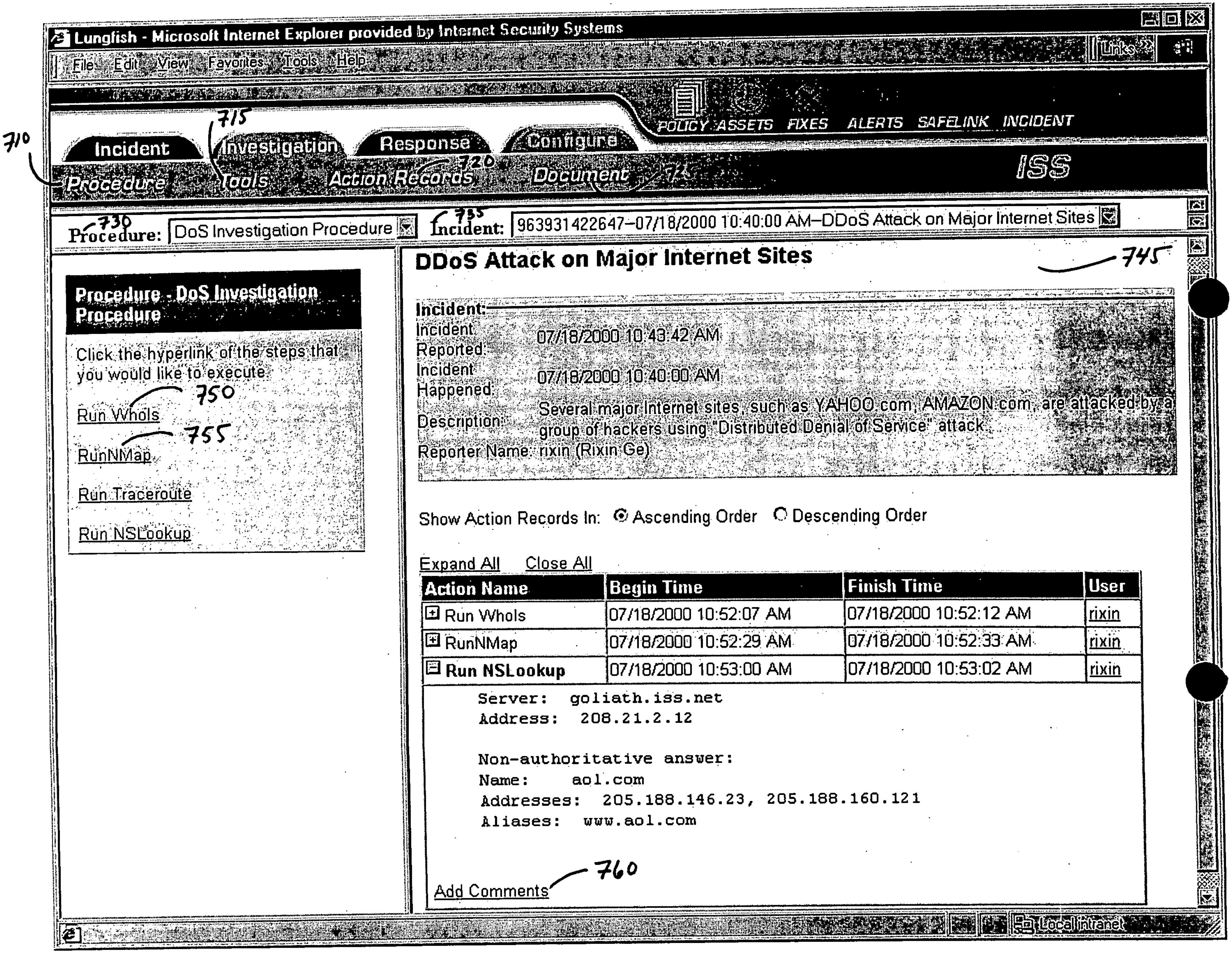

Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
POLICY ASSETS FIXES ALERTS SAFELINK INCIDEN
440
Incident
Investigation
Response
Configure
Report
View
Search
Edit
ISS
605
610
615
Done
Local intranet

Search Results

You can click on the Incident ID to edit the incident, click on the Incident Name to view the incident.

ID	Status	Incident Name	Incident Date	Report Date
954520331553	In Investigation	Test Incident1	03/01/2000 05:57:00 PM	03/31/2000 11:32:11 AM
955994401480	New	DDoS Attack onEBay.com	04/17/2000 01:52:03 PM	04/17/2000 02:00:01 PM
956002249963	New	Test Incident	04/17/2000 04:09:39 PM	04/17/2000 04:10:49 PM
956149177445	New	Test Apache	04/19/2000 08:55:00 AM	04/19/2000 08:59:37 AM
956172292063	New	Test Apache	04/19/2000 08:55:00 AM	04/19/2000 03:24:52 PM
956172334183	New	Test Apache	04/19/2000 08:55:00 AM	04/19/2000 03:25:34 PM
956174666357	New	Alert Test Again	04/19/2000 04:03:00 AM	04/19/2000 04:04:26 PM
959981258675	New	testsecurity	06/02/2000 05:26:00 AM	06/02/2000 05:27:38 PM
963410616255	New	Test IncidentHandler	07/01/2000 10:02:00 AM	07/12/2000 10:03:36 AM
963414077562	New	Denial of Service Attack 3	07/01/2000 11:00:00 AM	07/12/2000 11:01:17 AM
963927374185	In Investigation	DDoS Attack on Major Internet Sites	07/18/2000 09:32:00 AM	07/18/2000 09:36:14 AM
963929615578	In Investigation	DDoS Attack on Major Internet Sites	07/18/2000 10:10:00 AM	07/18/2000 10:13:35 AM
963931422647	In Investigation	DDoS Attack on Major Internet Sites	07/18/2000 10:40:00 AM	07/18/2000 10:43:42 AM

Fig. 6


Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
POLICY ASSETS FIXES ALERTS SAFELINK INCIDENT
Incident
Investigation
Response
Configure
Procedure
Tools
Action Records
Document
ISS
710
715
720
725
730
735
745
750
755
760
Local intranet

Procedure: DoS Investigation Procedure

Incident: 963931422647–07/18/2000 10:40:00 AM–DDoS Attack on Major Internet Sites

Procedure - DoS Investigation Procedure

Click the hyperlink of the steps that you would like to execute

Run WhoIs

RunNMap

Run Traceroute

Run NSLookup

DDoS Attack on Major Internet Sites

Incident:

Incident Reported:	07/18/2000 10:43:42 AM
Incident Happened:	07/18/2000 10:40:00 AM
Description:	Several major Internet sites, such as YAHOO.com, AMAZON.com, are attacked by a group of hackers using "Distributed Denial of Service" attack.
Reporter Name:	rixin (Rixin Ge)

Show Action Records In: ● Ascending Order ○ Descending Order

Expand All Close All

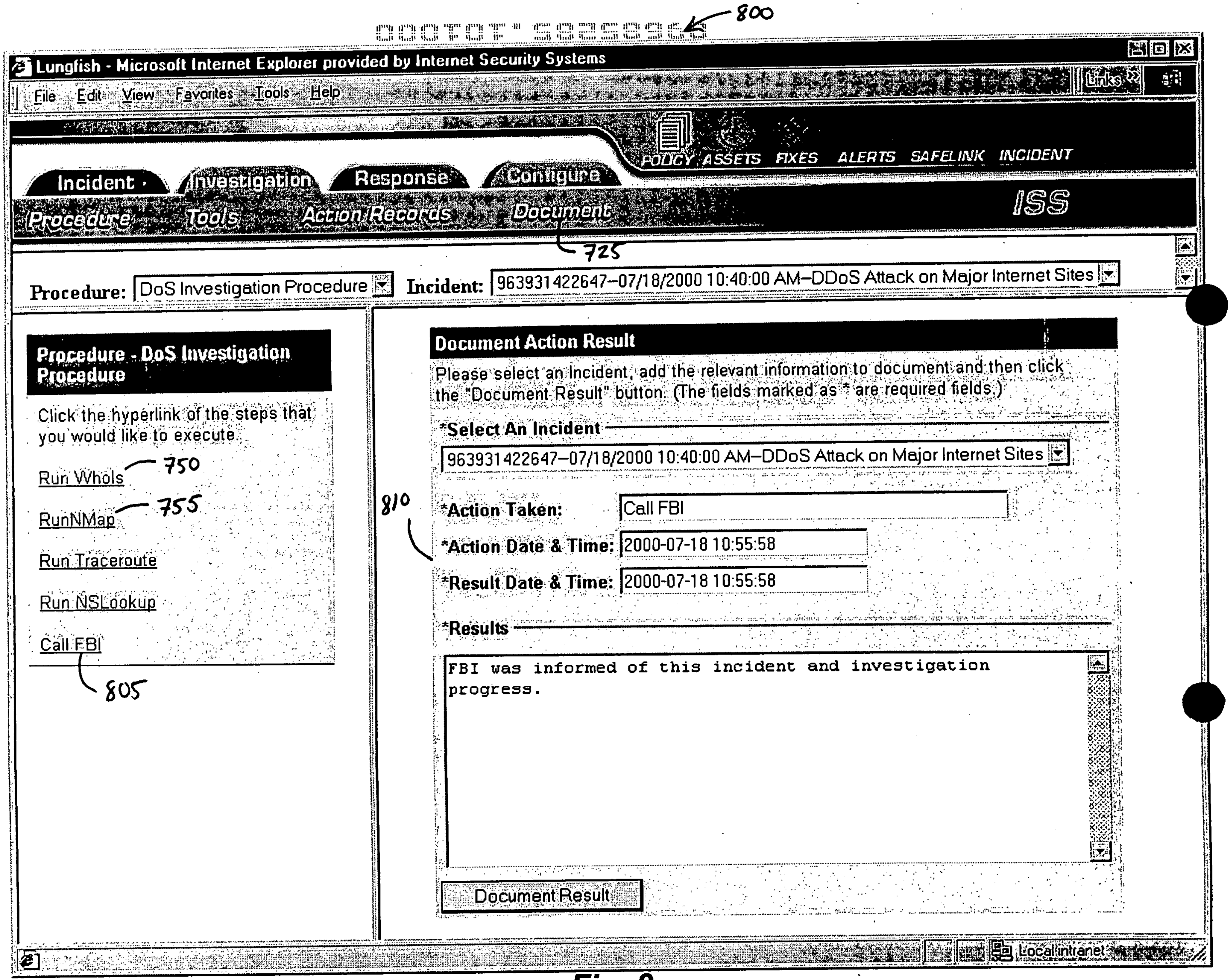
Action Name	Begin Time	Finish Time	User
⊞ Run WhoIs	07/18/2000 10:52:07 AM	07/18/2000 10:52:12 AM	rixin
⊞ RunNMap	07/18/2000 10:52:29 AM	07/18/2000 10:52:33 AM	rixin
⊟ **Run NSLookup**	07/18/2000 10:53:00 AM	07/18/2000 10:53:02 AM	rixin

```
Server:  goliath.iss.net
Address:  208.21.2.12

Non-authoritative answer:
Name:    aol.com
Addresses:  205.188.146.23, 205.188.160.121
Aliases:  www.aol.com
```

Add Comments

Fig. 7


800
Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
POLICY ASSETS FIXES ALERTS SAFELINK INCIDENT
Incident
Investigation
Response
Configure
Procedure
Tools
Action Records
Document
ISS
725
750
755
805
810
Document Result
Local intranet

Procedure: DoS Investigation Procedure

Incident: 963931422647–07/18/2000 10:40:00 AM–DDoS Attack on Major Internet Sites

Procedure - DoS Investigation Procedure

Click the hyperlink of the steps that you would like to execute.

Run WhoIs

RunNMap

Run Traceroute

Run NSLookup

Call FBI

Document Action Result

Please select an Incident, add the relevant information to document and then click the "Document Result" button. (The fields marked as * are required fields.)

*Select An Incident
963931422647–07/18/2000 10:40:00 AM–DDoS Attack on Major Internet Sites

*Action Taken: Call FBI

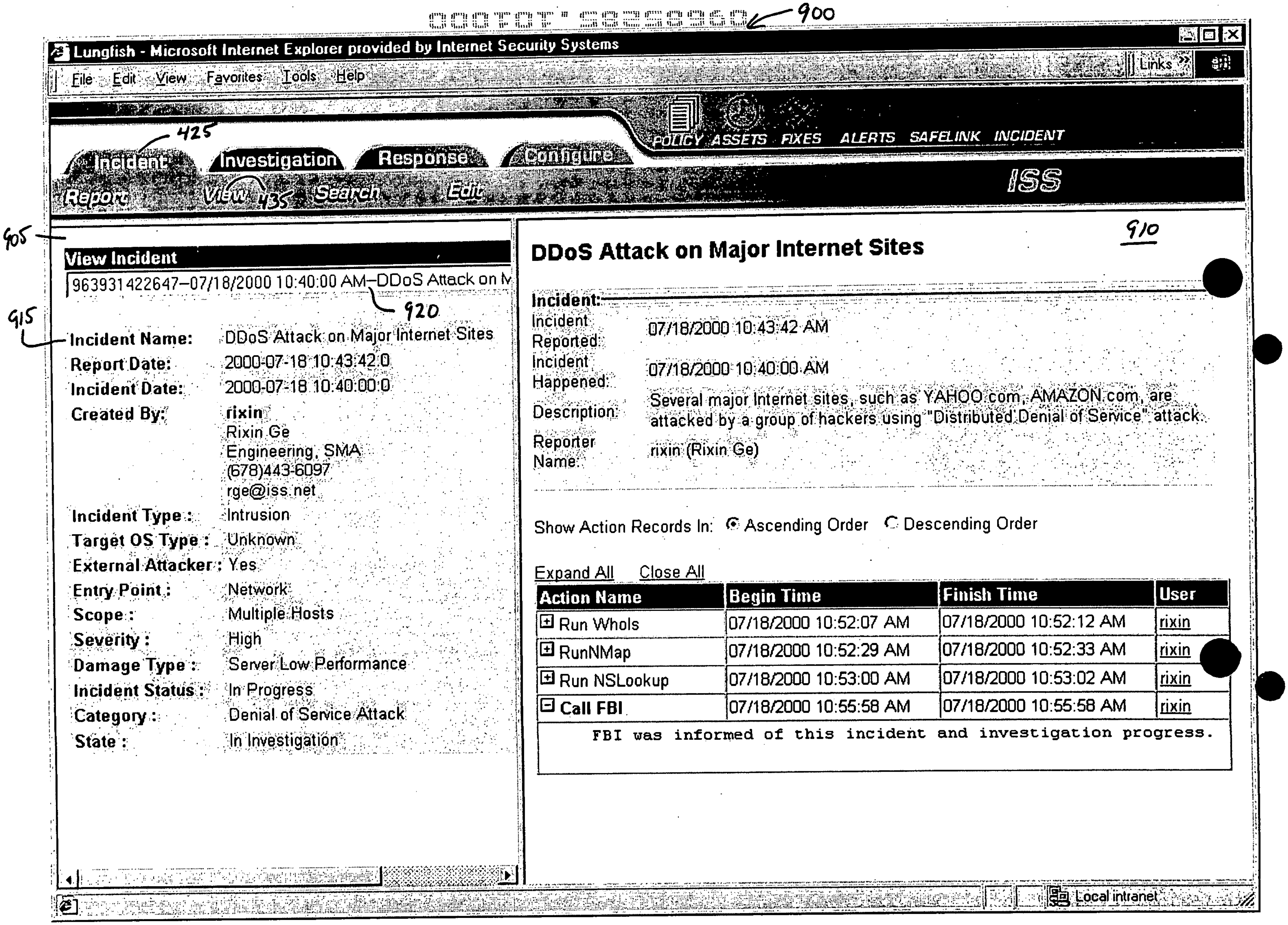
*Action Date & Time: 2000-07-18 10:55:58

*Result Date & Time: 2000-07-18 10:55:58

*Results

```
FBI was informed of this incident and investigation
progress.
```

Fig. 8



View Incident

963931422647–07/18/2000 10:40:00 AM–DDoS Attack on M

Incident Name:	DDoS Attack on Major Internet Sites
Report Date:	2000-07-18 10:43:42.0
Incident Date:	2000-07-18 10:40:00.0
Created By:	**rixin** Rixin Ge Engineering, SMA (678)443-6097 rge@iss.net
Incident Type :	Intrusion
Target OS Type :	Unknown
External Attacker :	Yes
Entry Point :	Network
Scope :	Multiple Hosts
Severity :	High
Damage Type :	Server Low Performance
Incident Status :	In Progress
Category :	Denial of Service Attack
State :	In Investigation

DDoS Attack on Major Internet Sites

Incident:

Incident Reported:	07/18/2000 10:43:42 AM
Incident Happened:	07/18/2000 10:40:00 AM
Description:	Several major Internet sites, such as YAHOO.com, AMAZON.com, are attacked by a group of hackers using "Distributed Denial of Service" attack.
Reporter Name:	rixin (Rixin Ge)

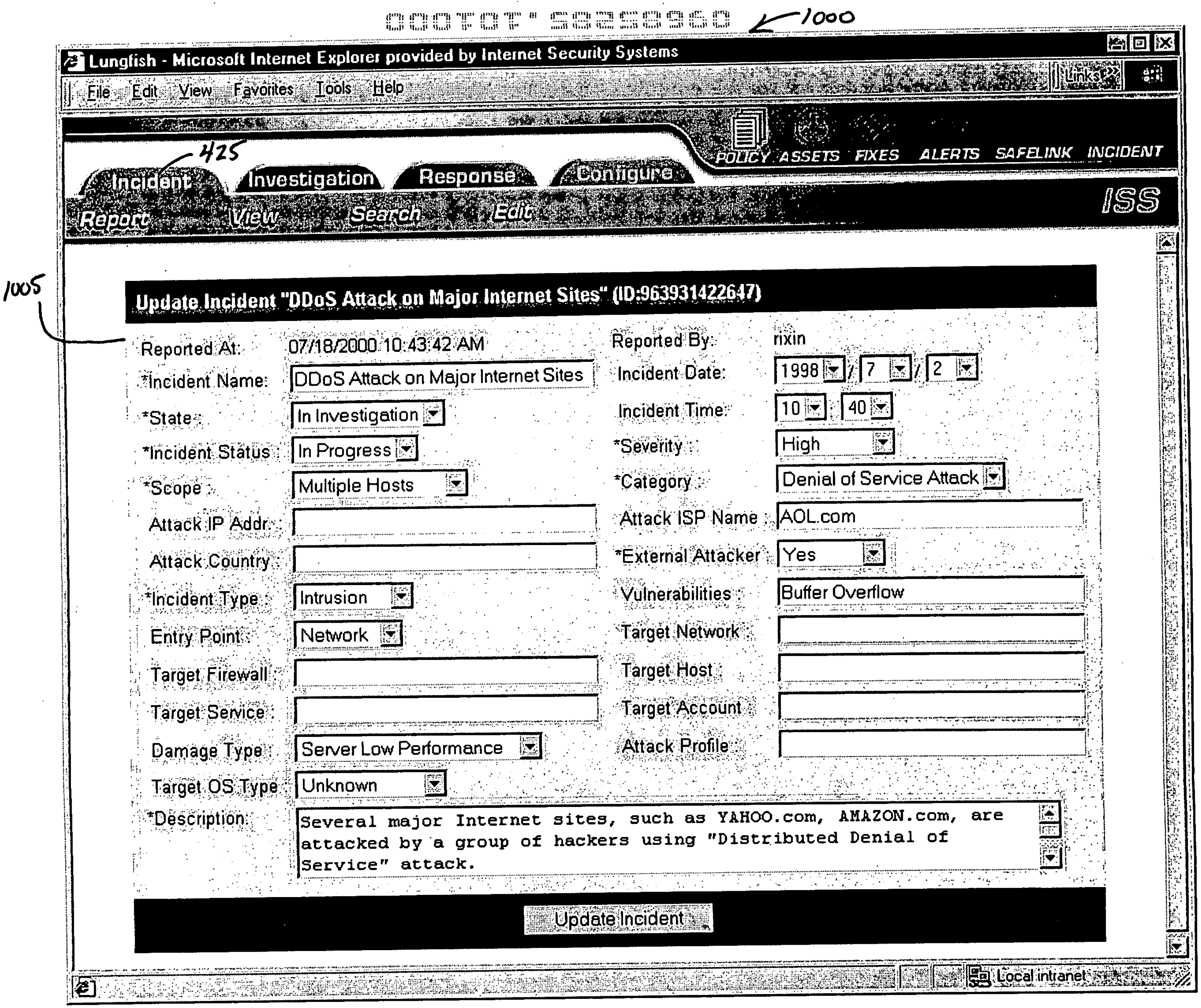
Show Action Records In: ◉ Ascending Order ○ Descending Order

Expand All Close All

Action Name	Begin Time	Finish Time	User
⊞ Run WhoIs	07/18/2000 10:52:07 AM	07/18/2000 10:52:12 AM	rixin
⊞ RunNMap	07/18/2000 10:52:29 AM	07/18/2000 10:52:33 AM	rixin
⊞ Run NSLookup	07/18/2000 10:53:00 AM	07/18/2000 10:53:02 AM	rixin
⊟ **Call FBI**	07/18/2000 10:55:58 AM	07/18/2000 10:55:58 AM	rixin

```
FBI was informed of this incident and investigation progress.
```

Fig. 9


1000
Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
POLICY ASSETS FIXES ALERTS SAFELINK INCIDENT
425
Incident Investigation Response Configure
Report View Search Edit
ISS
1005
Update Incident
Local intranet

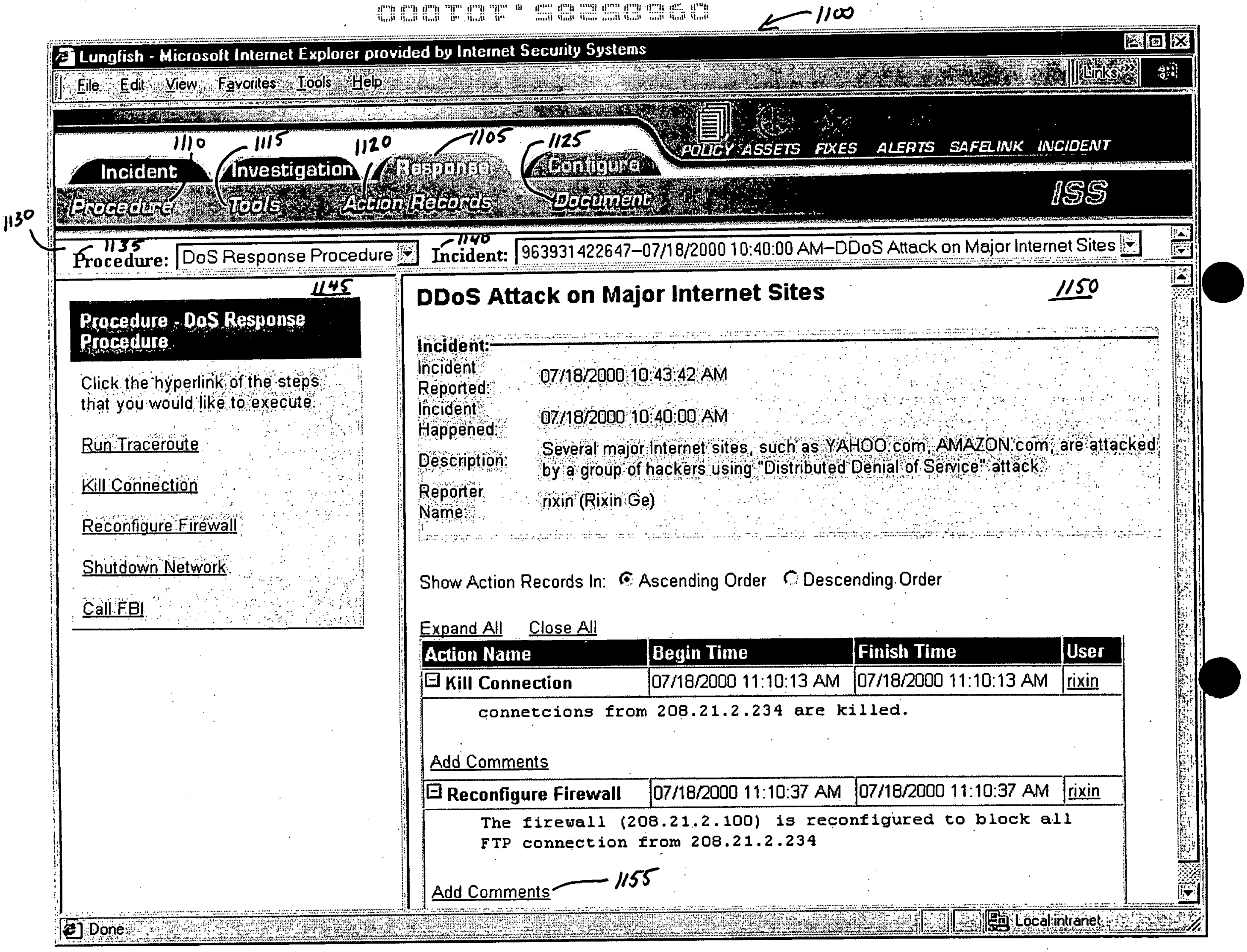
Update Incident "DDoS Attack on Major Internet Sites" (ID:963931422647)

Reported At:	07/18/2000 10:43:42 AM	Reported By:	rixin
*Incident Name:	DDoS Attack on Major Internet Sites	Incident Date:	1998 / 7 / 2
*State:	In Investigation	Incident Time:	10 40
*Incident Status:	In Progress	*Severity:	High
*Scope:	Multiple Hosts	*Category:	Denial of Service Attack
Attack IP Addr:		Attack ISP Name:	AOL.com
Attack Country:		*External Attacker:	Yes
*Incident Type:	Intrusion	Vulnerabilities:	Buffer Overflow
Entry Point:	Network	Target Network:	
Target Firewall:		Target Host:	
Target Service:		Target Account:	
Damage Type:	Server Low Performance	Attack Profile:	
Target OS Type:	Unknown		

*Description:

```
Several major Internet sites, such as YAHOO.com, AMAZON.com, are
attacked by a group of hackers using "Distributed Denial of
Service" attack.
```

Fig. 10


1100
1110
1115
1120
1105
1125
1130
1135
1140
1145
1150
1155
Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
Incident
Investigation
Response
Configure
Procedure
Tools
Action Records
Document
POLICY ASSETS FIXES ALERTS SAFELINK INCIDENT
ISS
Done
Local intranet

Procedure: DoS Response Procedure

Incident: 963931422647–07/18/2000 10:40:00 AM–DDoS Attack on Major Internet Sites

Procedure - DoS Response Procedure

Click the hyperlink of the steps that you would like to execute

Run Traceroute

Kill Connection

Reconfigure Firewall

Shutdown Network

Call FBI

DDoS Attack on Major Internet Sites

Incident:

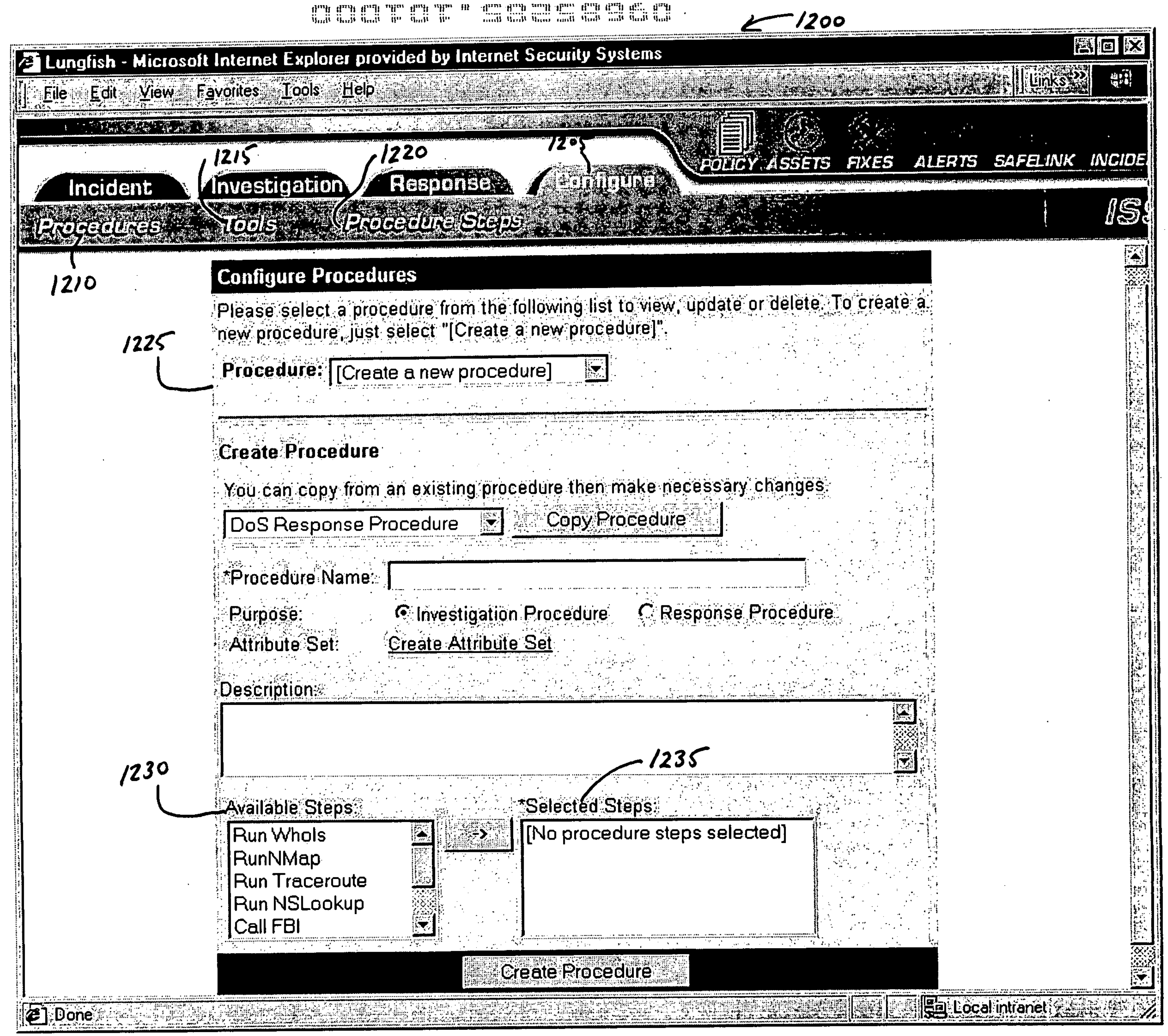
Incident Reported:	07/18/2000 10:43:42 AM
Incident Happened:	07/18/2000 10:40:00 AM
Description:	Several major Internet sites, such as YAHOO.com, AMAZON.com, are attacked by a group of hackers using "Distributed Denial of Service" attack.
Reporter Name:	rixin (Rixin Ge)

Show Action Records In: ● Ascending Order ○ Descending Order

Expand All Close All

Action Name	Begin Time	Finish Time	User
⊟ Kill Connection	07/18/2000 11:10:13 AM	07/18/2000 11:10:13 AM	rixin
connetcions from 208.21.2.234 are killed. Add Comments			
⊟ Reconfigure Firewall	07/18/2000 11:10:37 AM	07/18/2000 11:10:37 AM	rixin
The firewall (208.21.2.100) is reconfigured to block all FTP connection from 208.21.2.234 Add Comments			

Fig. 11


1200
Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links
POLICY ASSETS FIXES ALERTS SAFELINK INCIDE
Incident
Investigation
Response
Configure
Procedures
Tools
Procedure Steps
1215
1220
1205
1210
1225
1230
1235
Done
Local intranet

Configure Procedures

Please select a procedure from the following list to view, update or delete. To create a new procedure, just select "[Create a new procedure]".

Procedure: [Create a new procedure]

Create Procedure

You can copy from an existing procedure then make necessary changes.

DoS Response Procedure | Copy Procedure

*Procedure Name:

Purpose: ● Investigation Procedure ○ Response Procedure

Attribute Set: Create Attribute Set

Description:

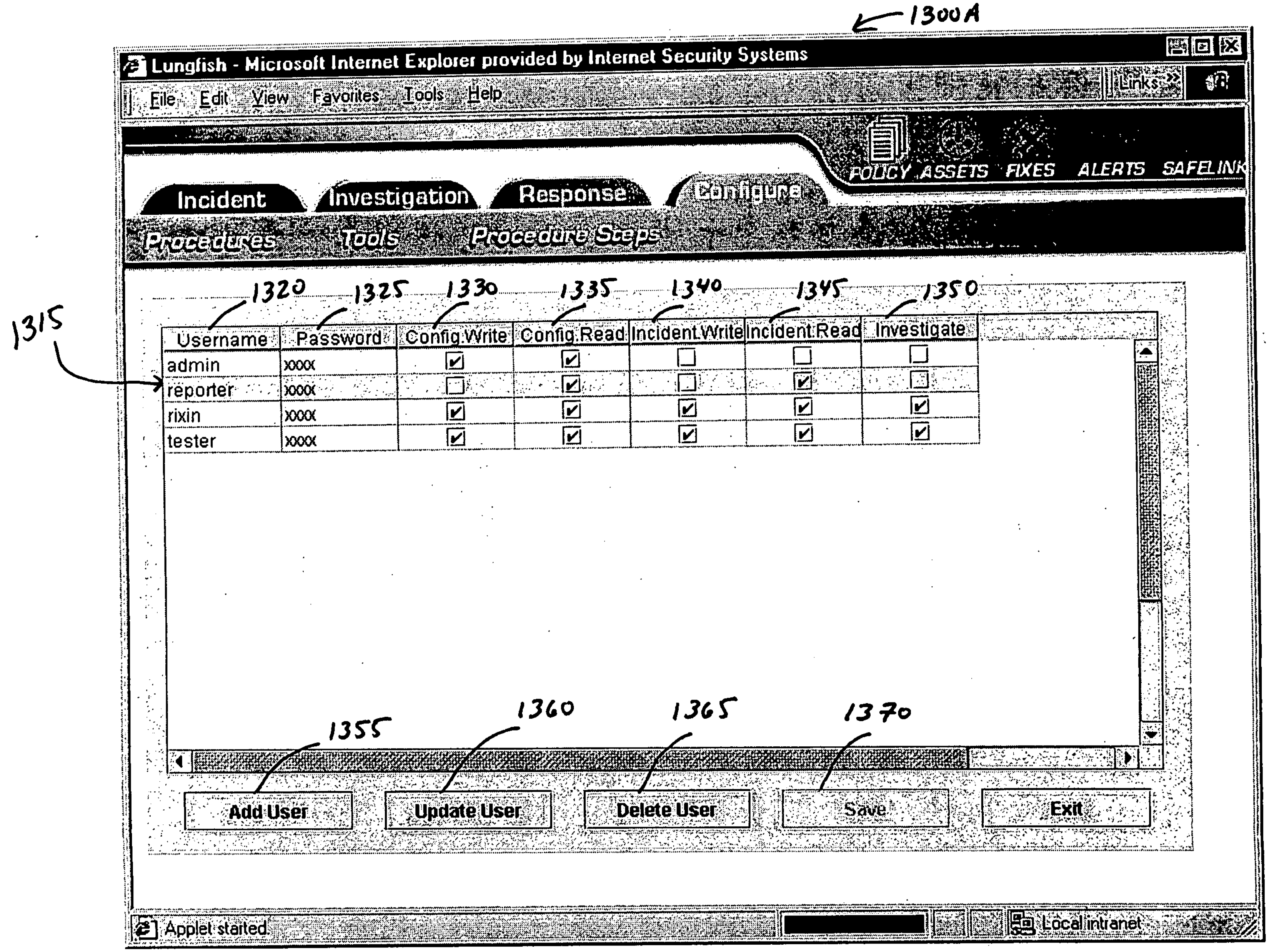
Available Steps:
- Run WhoIs
- RunNMap
- Run Traceroute
- Run NSLookup
- Call FBI

->

*Selected Steps:
[No procedure steps selected]

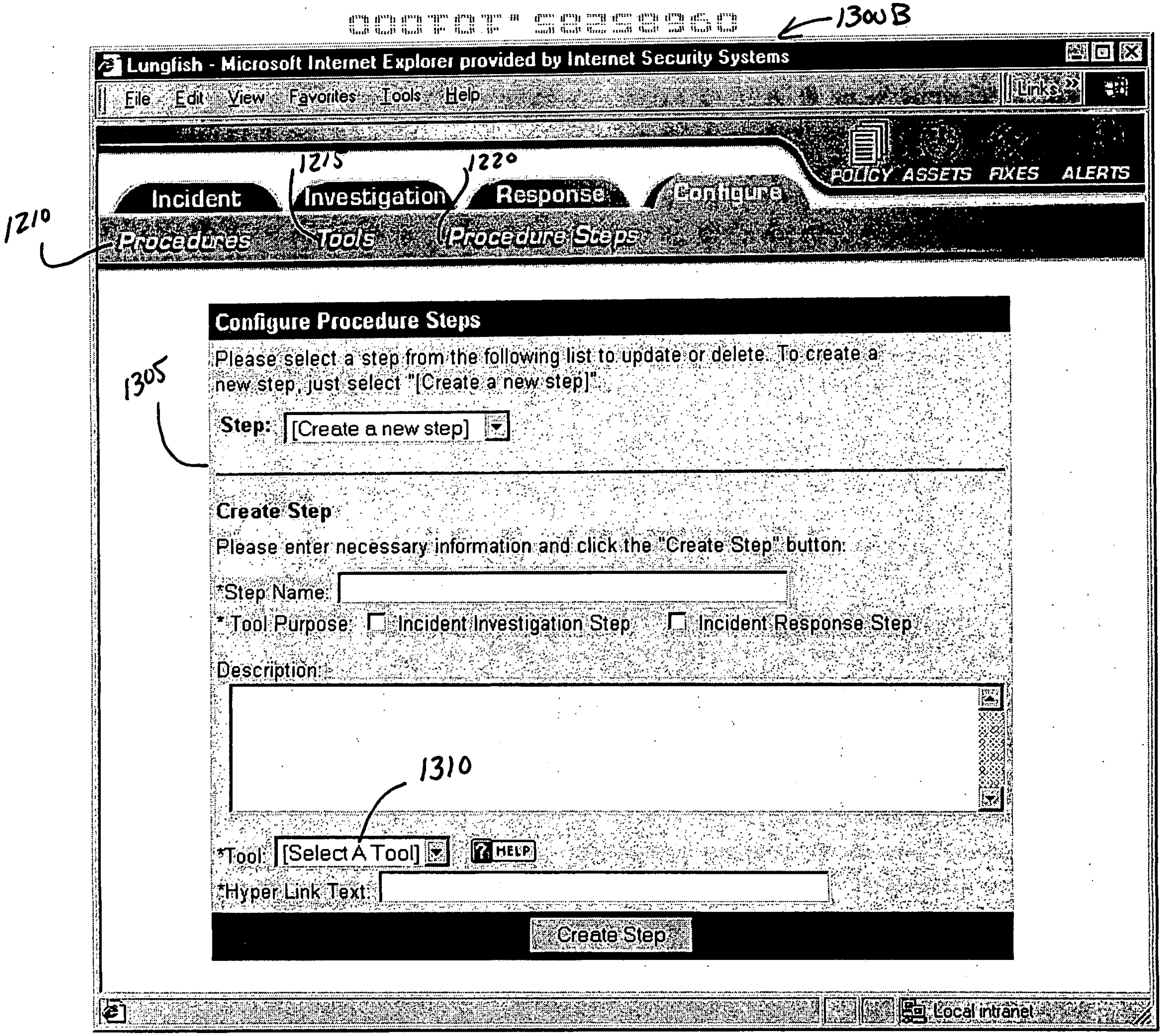
Create Procedure

Fig. 12



Username	Password	Config.Write	Config.Read	Incident.Write	Incident.Read	Investigate
admin	xxxx	☑	☑	□	□	□
reporter	xxxx	□	☑	□	☑	□
rixin	xxxx	☑	☑	☑	☑	☑
tester	xxxx	☑	☑	☑	☑	☑

Fig. 13A



Lungfish - Microsoft Internet Explorer provided by Internet Security Systems

Configure Procedure Steps

Please select a step from the following list to update or delete. To create a new step, just select "[Create a new step]".

Step: [Create a new step]

Create Step

Please enter necessary information and click the "Create Step" button:

*Step Name:

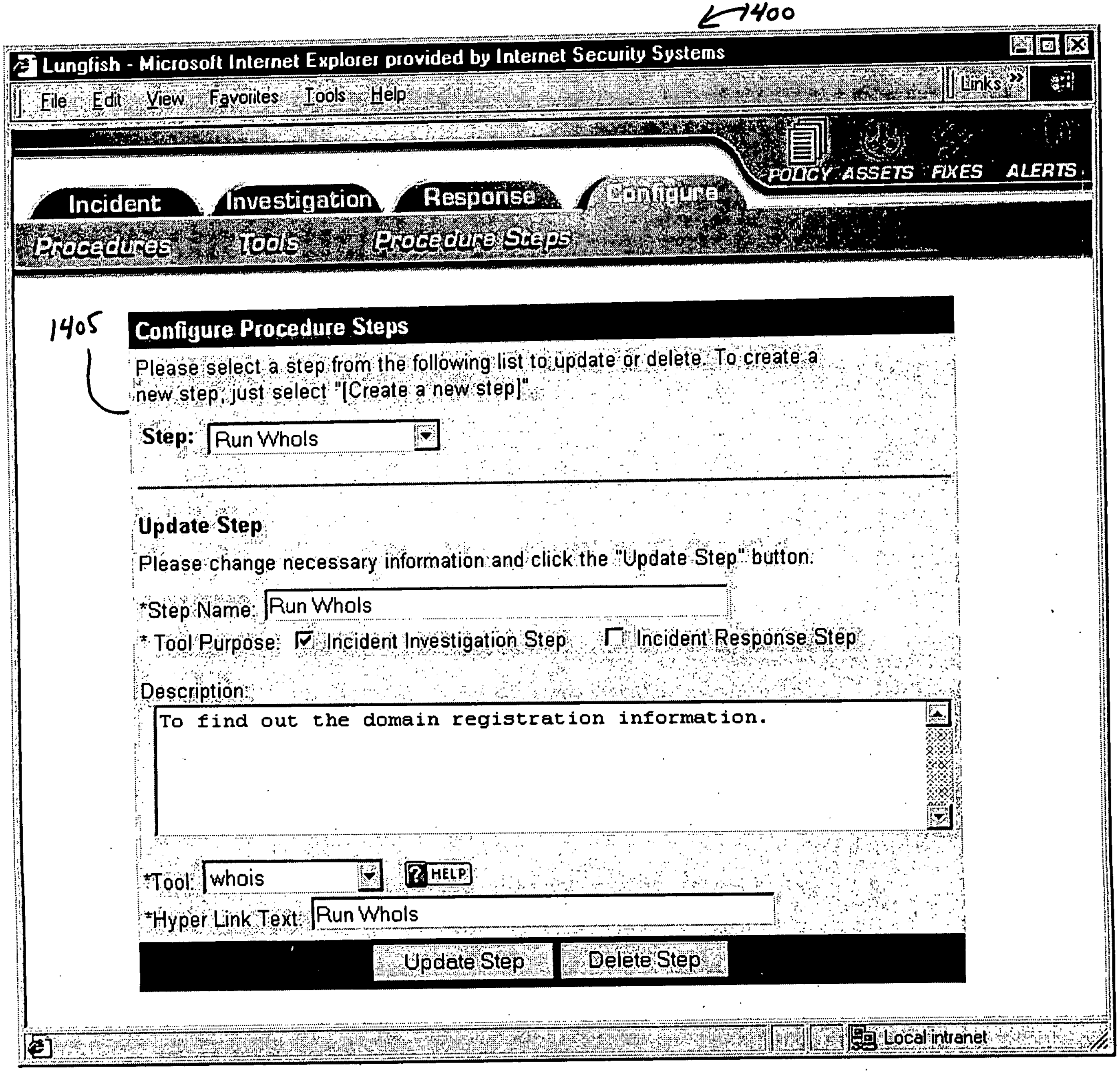
*Tool Purpose: □ Incident Investigation Step □ Incident Response Step

Description:

*Tool: [Select A Tool]

*Hyper Link Text:

Fig. 13B



Configure Procedure Steps

Please select a step from the following list to update or delete. To create a new step, just select "[Create a new step]".

Step: Run WhoIs

Update Step

Please change necessary information and click the "Update Step" button.

*Step Name: Run WhoIs

* Tool Purpose: ☑ Incident Investigation Step ☐ Incident Response Step

Description:

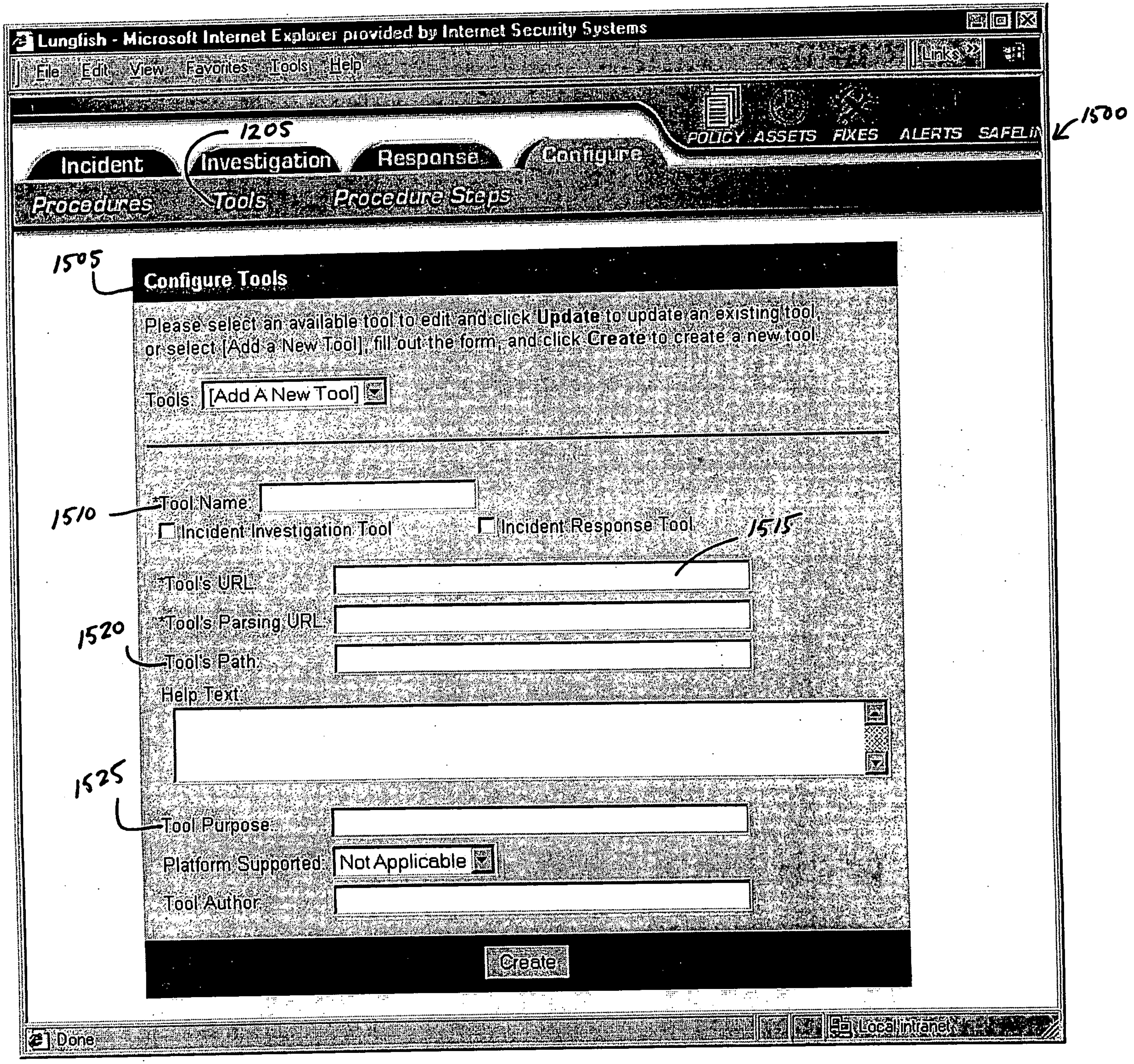
```
To find out the domain registration information.
```

*Tool: whois

*Hyper Link Text: Run WhoIs

Update Step | Delete Step

Fig. 14



Configure Tools

Please select an available tool to edit and click **Update** to update an existing tool, or select [Add a New Tool], fill out the form, and click **Create** to create a new tool.

Tools: [Add A New Tool]

*Tool Name:

□ Incident Investigation Tool □ Incident Response Tool

*Tool's URL:

*Tool's Parsing URL:

Tool's Path:

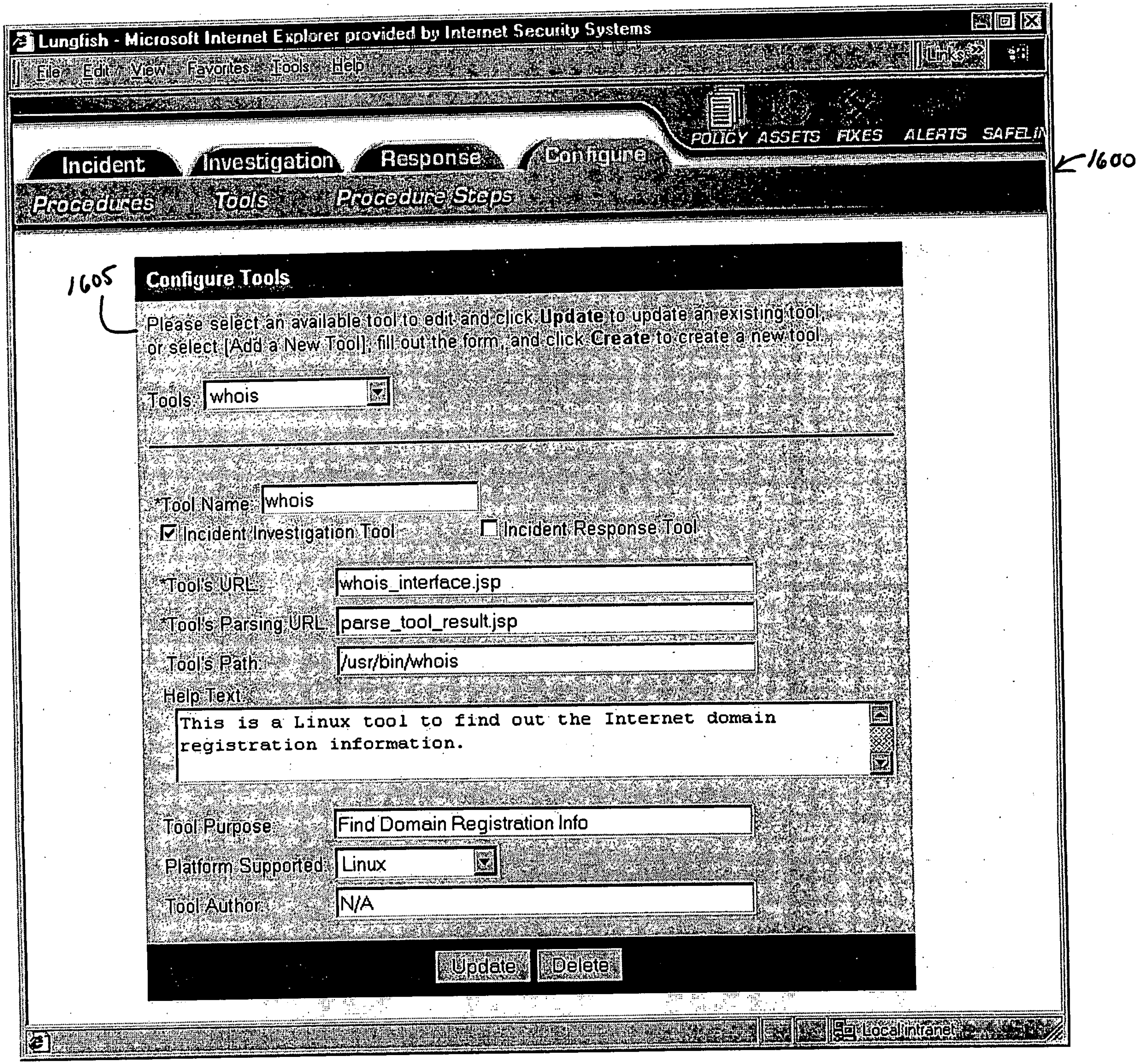
Help Text:

Tool Purpose:

Platform Supported: Not Applicable

Tool Author:

Fig. 15


Lungfish - Microsoft Internet Explorer provided by Internet Security Systems
File Edit View Favorites Tools Help
Links »
POLICY ASSETS FIXES ALERTS SAFELI
Incident
Investigation
Response
Configure
Procedures
Tools
Procedure Steps
1600
1605
Update
Delete
Local intranet

Configure Tools

Please select an available tool to edit and click **Update** to update an existing tool, or select [Add a New Tool], fill out the form, and click **Create** to create a new tool.

Tools: whois

*Tool Name: whois

☑ Incident Investigation Tool ☐ Incident Response Tool

*Tool's URL: whois_interface.jsp

*Tool's Parsing URL: parse_tool_result.jsp

Tool's Path: /usr/bin/whois

Help Text:

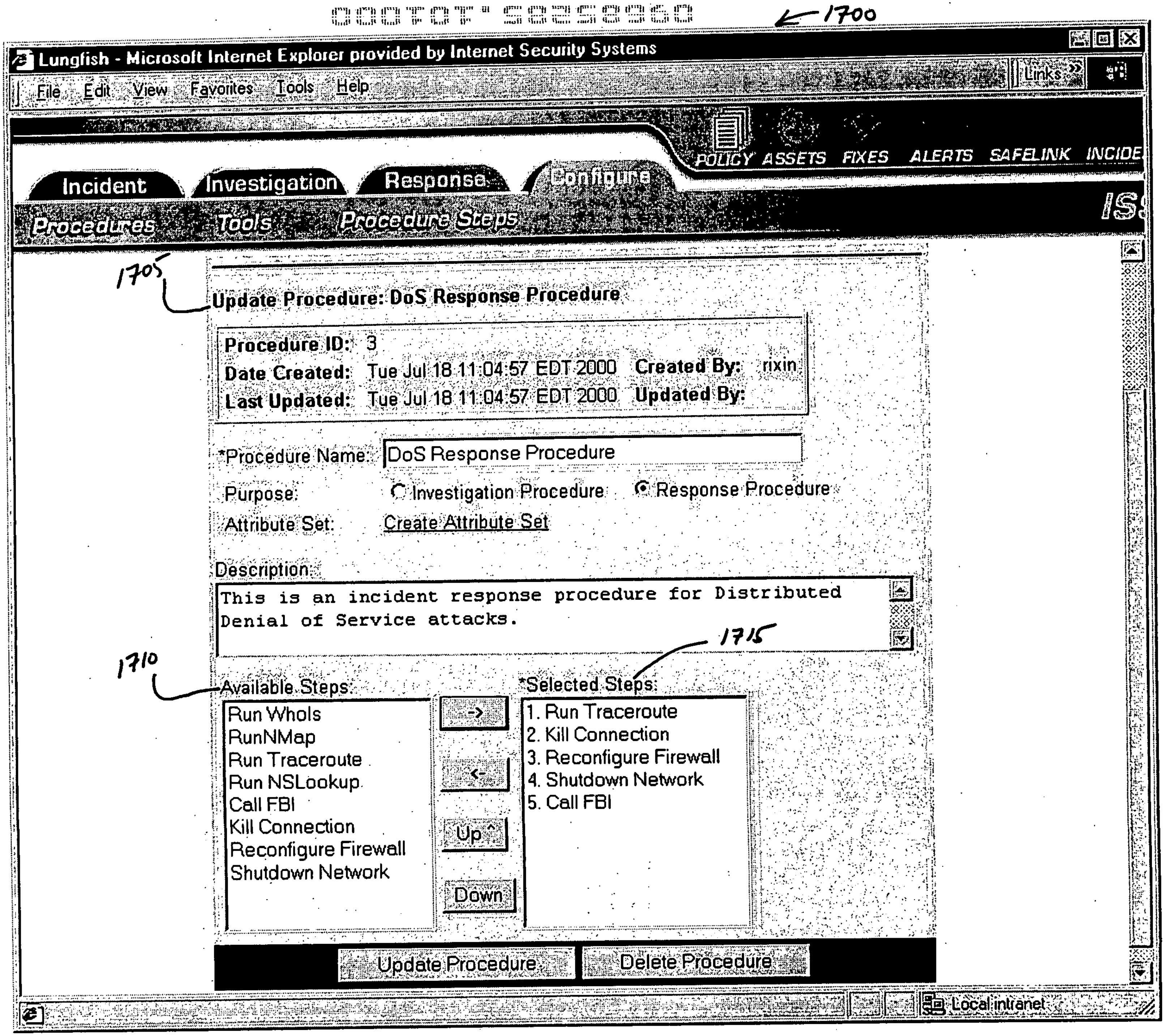
```
This is a Linux tool to find out the Internet domain
registration information.
```

Tool Purpose: Find Domain Registration Info

Platform Supported: Linux

Tool Author: N/A

Fig. 16



Update Procedure: DoS Response Procedure

Procedure ID: 3
Date Created: Tue Jul 18 11:04:57 EDT 2000 **Created By:** rixin
Last Updated: Tue Jul 18 11:04:57 EDT 2000 **Updated By:**

*Procedure Name: DoS Response Procedure

Purpose: ○ Investigation Procedure ● Response Procedure

Attribute Set: Create Attribute Set

Description:

```
This is an incident response procedure for Distributed
Denial of Service attacks.
```

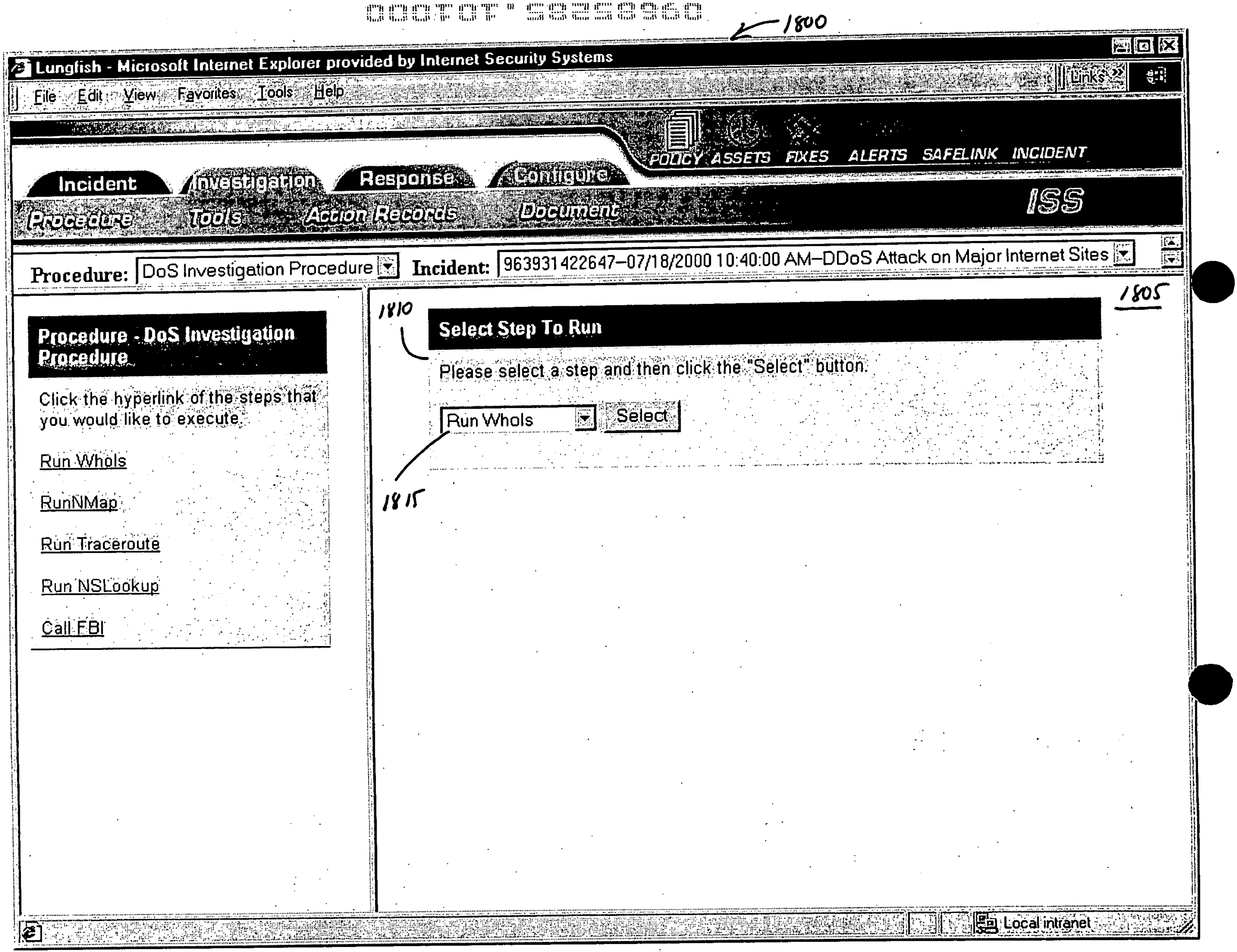
Available Steps:

Run WhoIs
RunNMap
Run Traceroute
Run NSLookup
Call FBI
Kill Connection
Reconfigure Firewall
Shutdown Network

*Selected Steps:

1. Run Traceroute
2. Kill Connection
3. Reconfigure Firewall
4. Shutdown Network
5. Call FBI

Fig. 17



Procedure: DoS Investigation Procedure **Incident:** 963931422647–07/18/2000 10:40:00 AM–DDoS Attack on Major Internet Sites

Procedure - DoS Investigation Procedure

Click the hyperlink of the steps that you would like to execute.

Run WhoIs

RunNMap

Run Traceroute

Run NSLookup

Call FBI

Select Step To Run

Please select a step and then click the "Select" button.

Run WhoIs ▾ Select

Fig. 18

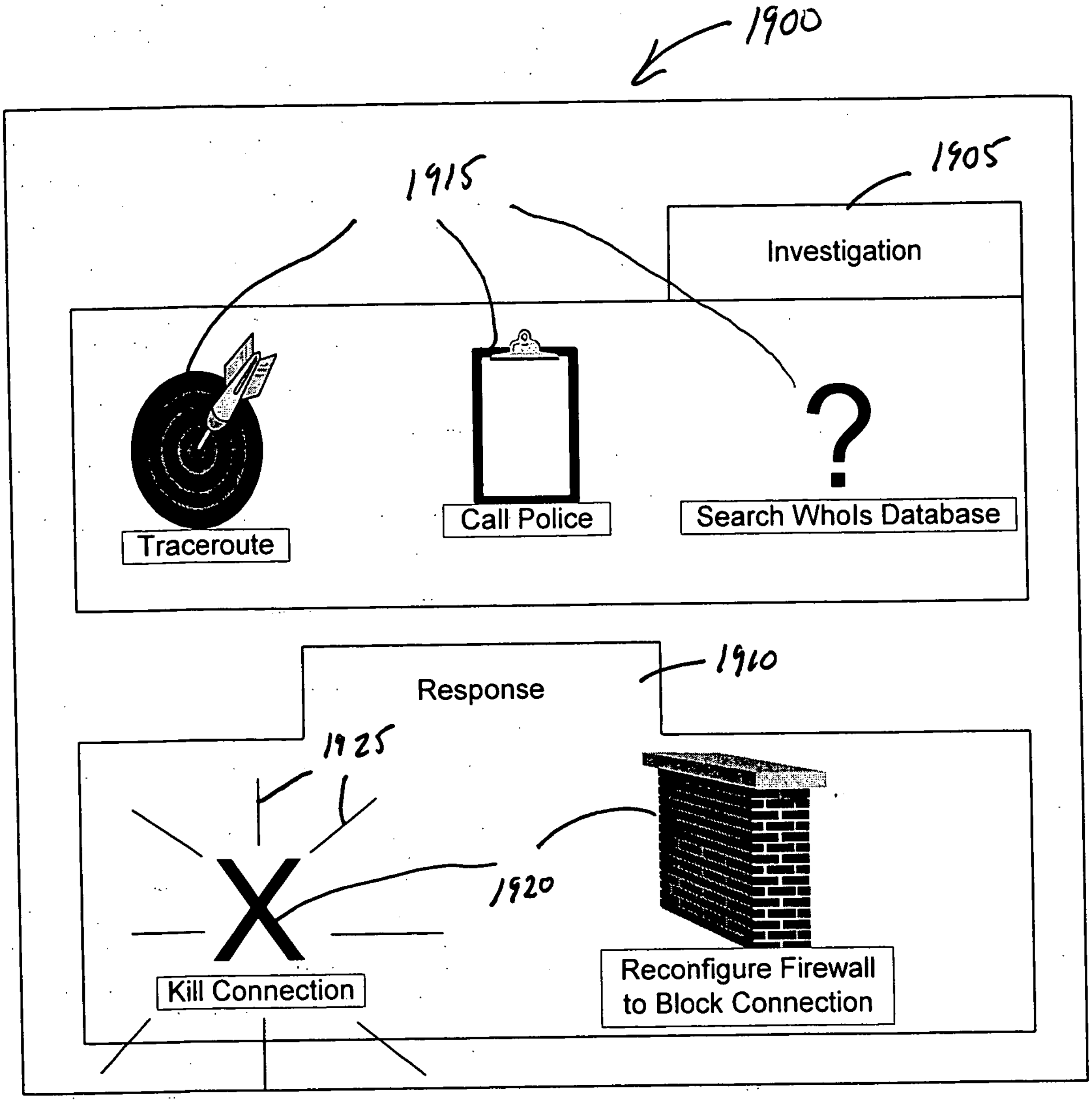
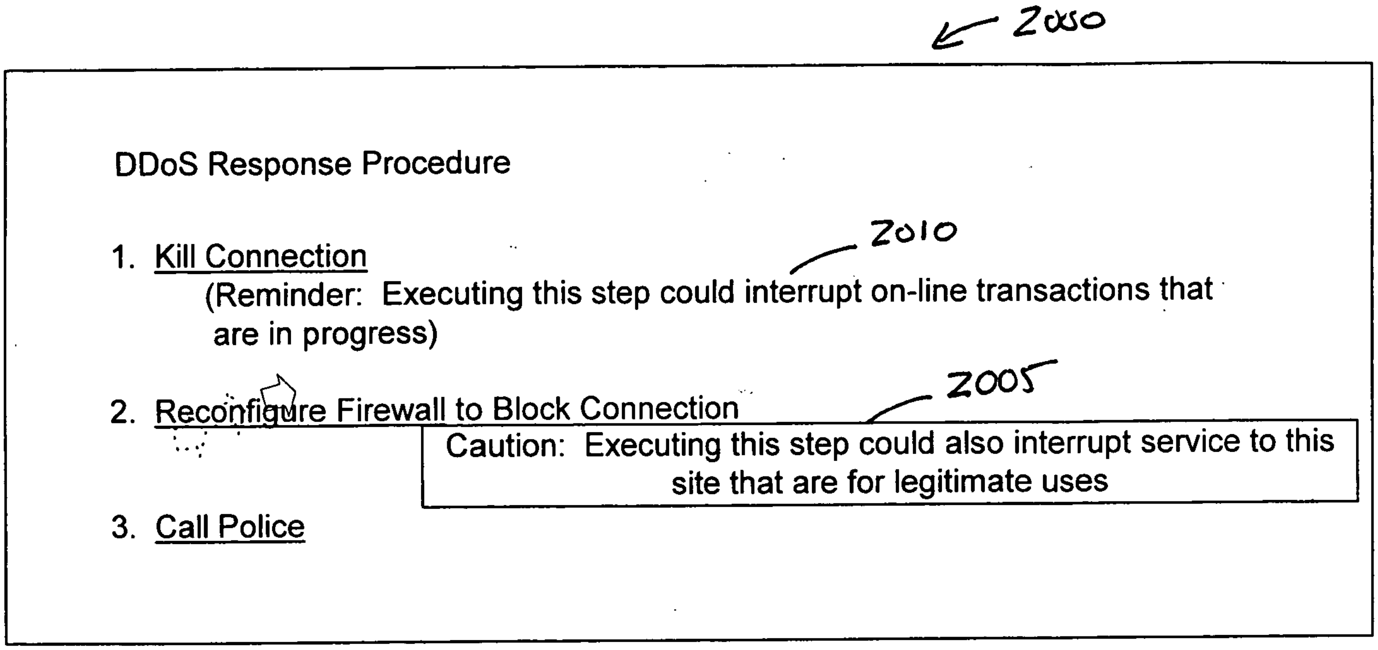

1900
1905
Investigation
1915
Traceroute
Call Police
Search WhoIs Database
Response
1910
1925
1920
Kill Connection
Reconfigure Firewall to Block Connection

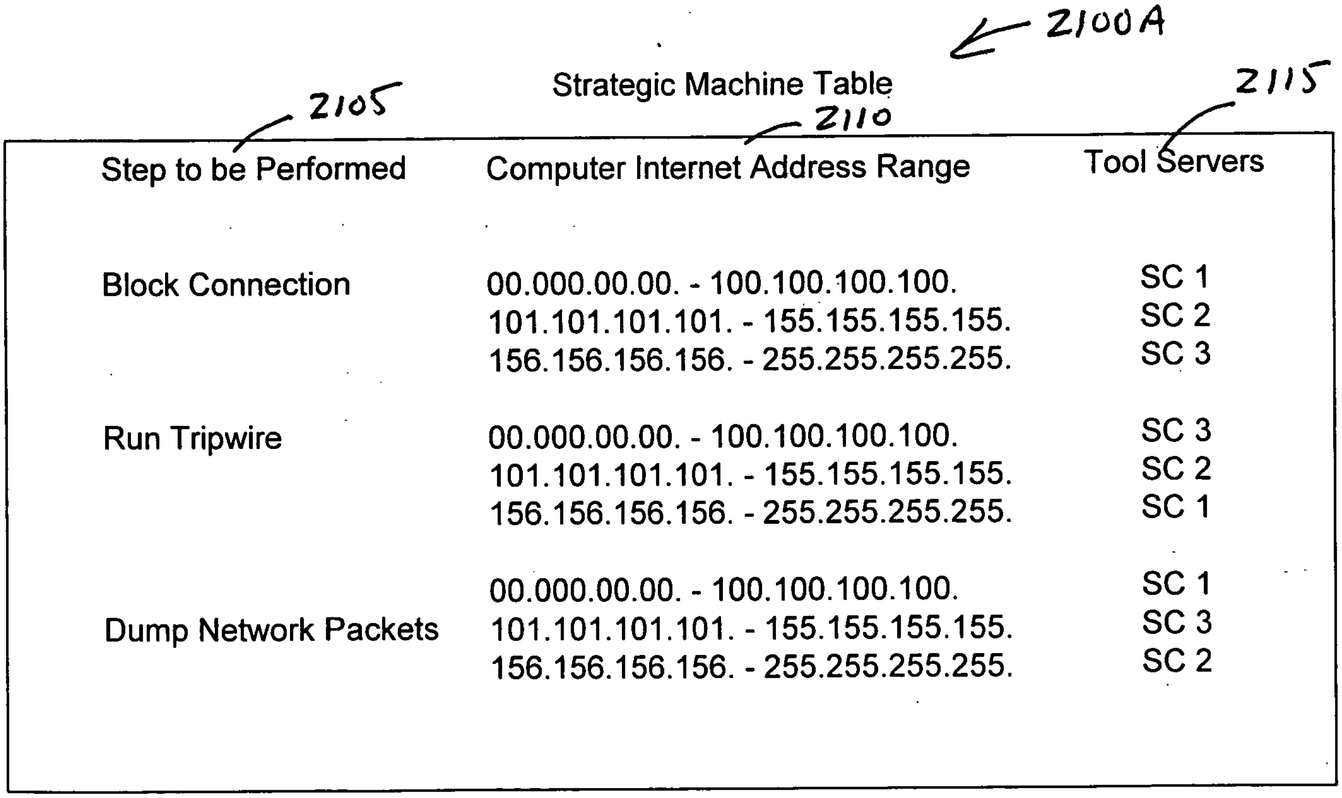
FIG. 19



DDoS Response Procedure

1. Kill Connection
   (Reminder: Executing this step could interrupt on-line transactions that are in progress)
2. Reconfigure Firewall to Block Connection
   Caution: Executing this step could also interrupt service to this site that are for legitimate uses
3. Call Police

FIG. 20


2100A
2105
2110
2115

Strategic Machine Table

Step to be Performed	Computer Internet Address Range	Tool Servers
Block Connection	00.000.00.00. - 100.100.100.100.	SC 1
	101.101.101.101. - 155.155.155.155.	SC 2
	156.156.156.156. - 255.255.255.255.	SC 3
Run Tripwire	00.000.00.00. - 100.100.100.100.	SC 3
	101.101.101.101. - 155.155.155.155.	SC 2
	156.156.156.156. - 255.255.255.255.	SC 1
Dump Network Packets	00.000.00.00. - 100.100.100.100.	SC 1
	101.101.101.101. - 155.155.155.155.	SC 3
	156.156.156.156. - 255.255.255.255.	SC 2

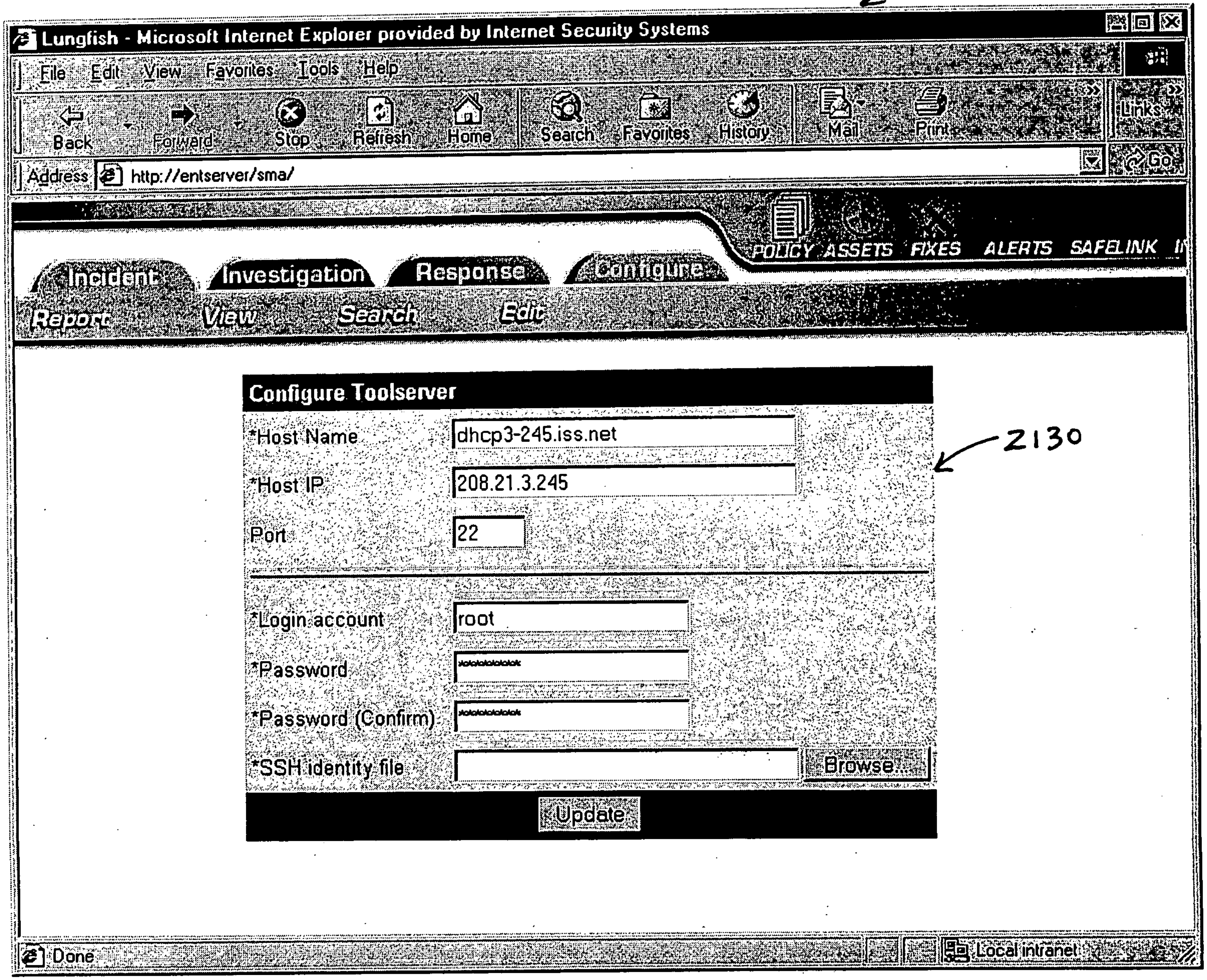
FIG. 21A

2700B

Security Agent	Status	Incident Name	Procedure Used	Incident Date	Procedure Start date	Incident Source	Target
Adams, James	Closed	DoS Attack on Firewall	DoS Response Procedure	11/15/99	11/25/99	123.456.789.909.	Yahoo!
Bastin, Knicole	In Response	DoS Attack on Corporate Web Server	Dos Response Procedure	11/15/99	11/29/99	455.326.8999.494.	AOL
Castle, Marie	In Response	Virus Attack on Accounting	Virus III Response	11/15/99	11/26/99	345.546.888.22.	Accounting
●	●	●	●	●	●	●	●
●	●	●	●	●	●	●	●
●	●	●	●	●	●	●	●

FIG. 21B

2100C



Configure Toolserver

*Host Name	dhcp3-245.iss.net
*Host IP	208.21.3.245
Port	22
*Login account	root
*Password	*********
*Password (Confirm)	*********
*SSH identity file	

Fig. 21C

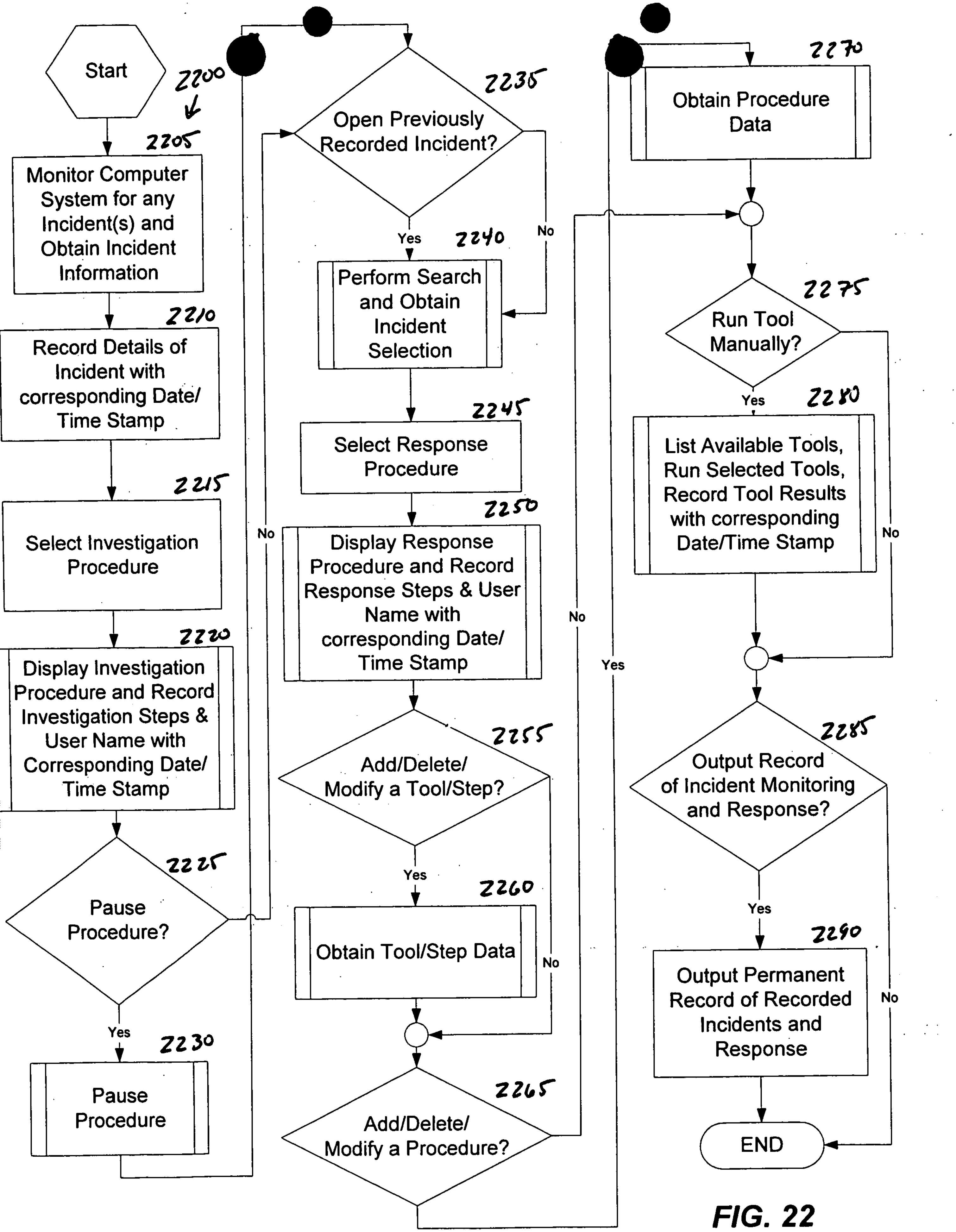

Start
2200
2205
Monitor Computer System for any Incident(s) and Obtain Incident Information
2210
Record Details of Incident with corresponding Date/ Time Stamp
2215
Select Investigation Procedure
2220
Display Investigation Procedure and Record Investigation Steps & User Name with Corresponding Date/ Time Stamp
2225
Pause Procedure?
Yes
No
2230
Pause Procedure
2235
Open Previously Recorded Incident?
Yes
No
2240
Perform Search and Obtain Incident Selection
2245
Select Response Procedure
2250
Display Response Procedure and Record Response Steps & User Name with corresponding Date/ Time Stamp
2255
Add/Delete/ Modify a Tool/Step?
Yes
No
2260
Obtain Tool/Step Data
2265
Add/Delete/ Modify a Procedure?
No
Yes
2270
Obtain Procedure Data
2275
Run Tool Manually?
Yes
No
2280
List Available Tools, Run Selected Tools, Record Tool Results with corresponding Date/Time Stamp
2285
Output Record of Incident Monitoring and Response?
Yes
No
2290
Output Permanent Record of Recorded Incidents and Response
END

FIG. 22

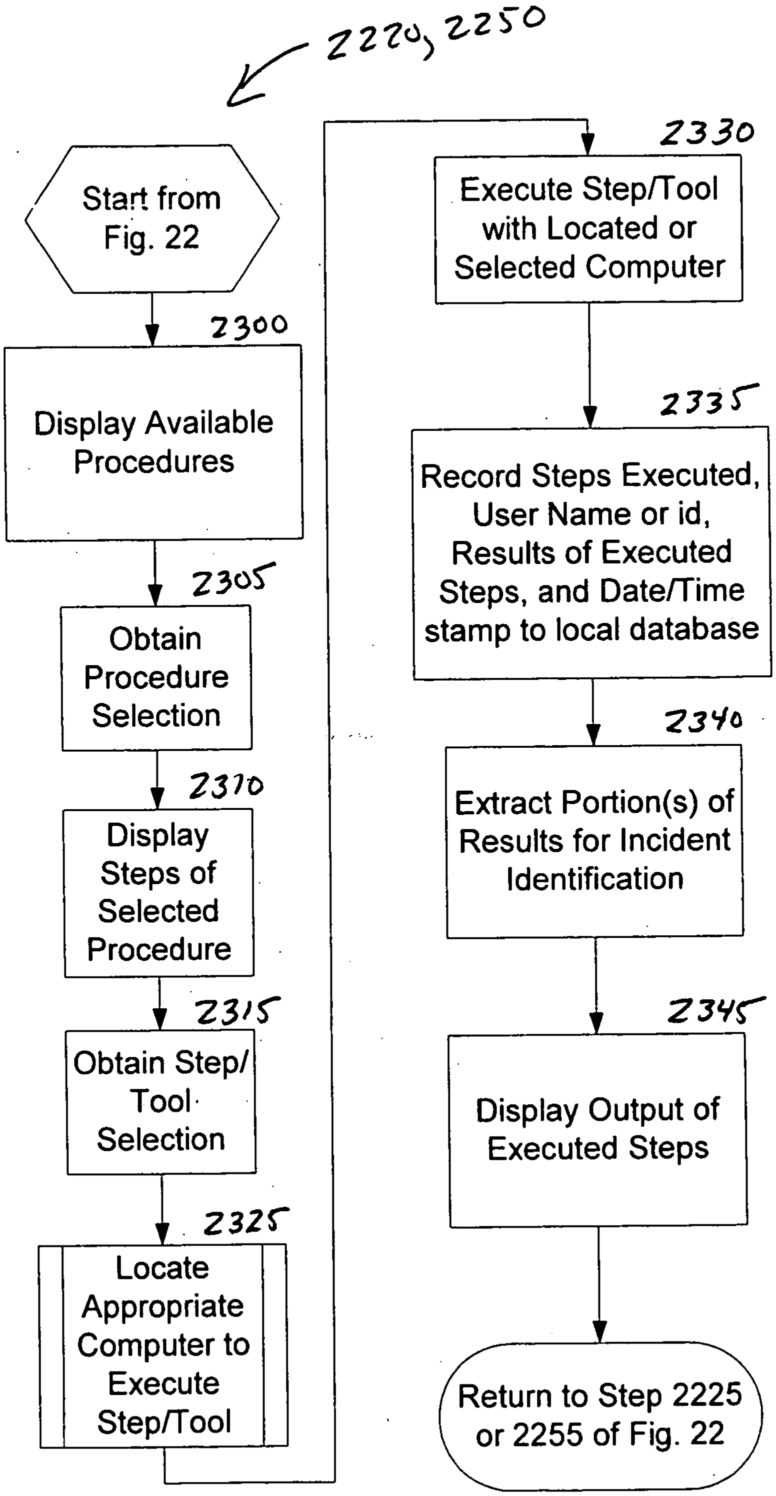

2220, 2250
Start from Fig. 22
2300
Display Available Procedures
2305
Obtain Procedure Selection
2310
Display Steps of Selected Procedure
2315
Obtain Step/ Tool Selection
2325
Locate Appropriate Computer to Execute Step/Tool
2330
Execute Step/Tool with Located or Selected Computer
2335
Record Steps Executed, User Name or id, Results of Executed Steps, and Date/Time stamp to local database
2340
Extract Portion(s) of Results for Incident Identification
2345
Display Output of Executed Steps
Return to Step 2225 or 2255 of Fig. 22

FIG. 23

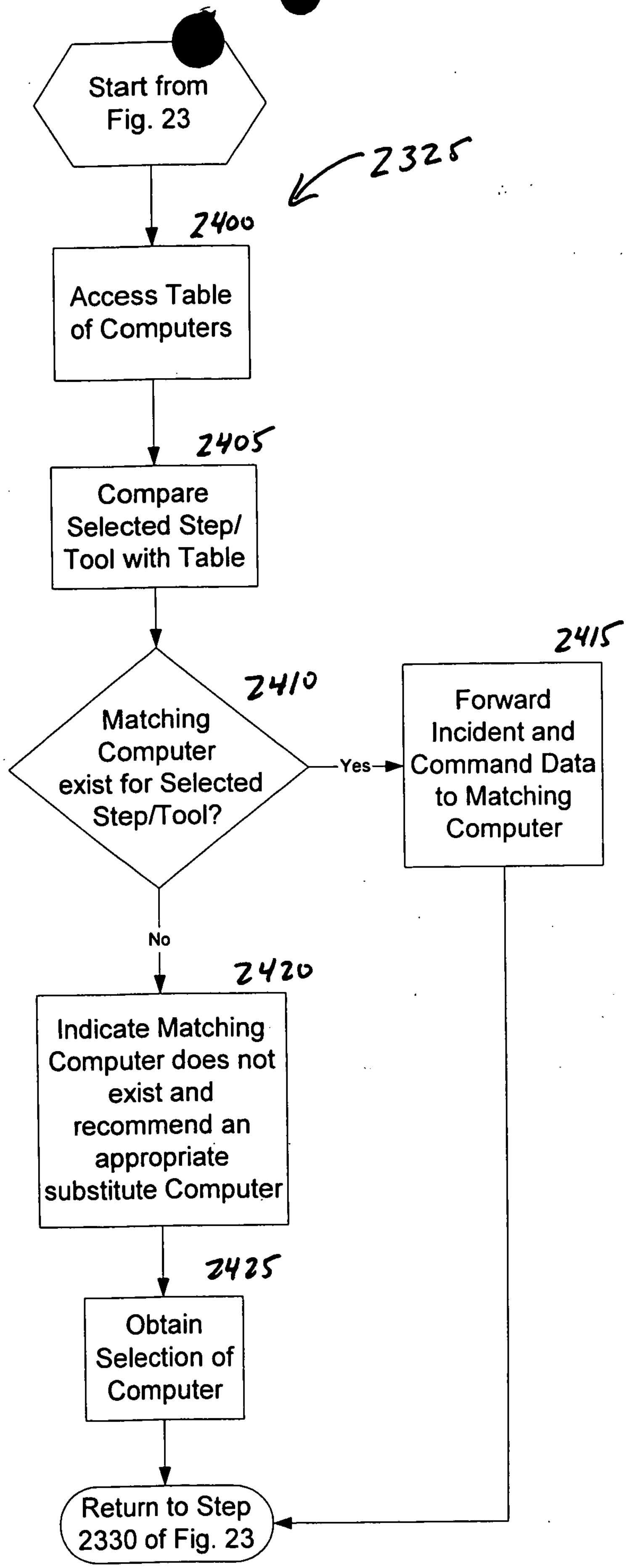

Start from Fig. 23
2325
2400
Access Table of Computers
2405
Compare Selected Step/ Tool with Table
2410
Matching Computer exist for Selected Step/Tool?
Yes
2415
Forward Incident and Command Data to Matching Computer
No
2420
Indicate Matching Computer does not exist and recommend an appropriate substitute Computer
2425
Obtain Selection of Computer
Return to Step 2330 of Fig. 23

FIG. 24

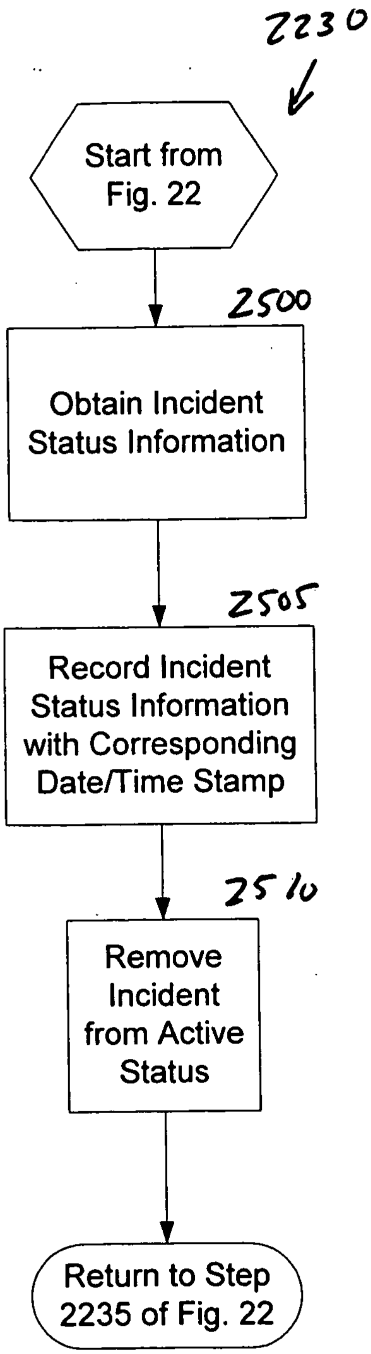

2230
Start from Fig. 22
2500
Obtain Incident Status Information
2505
Record Incident Status Information with Corresponding Date/Time Stamp
2510
Remove Incident from Active Status
Return to Step 2235 of Fig. 22

FIG. 25

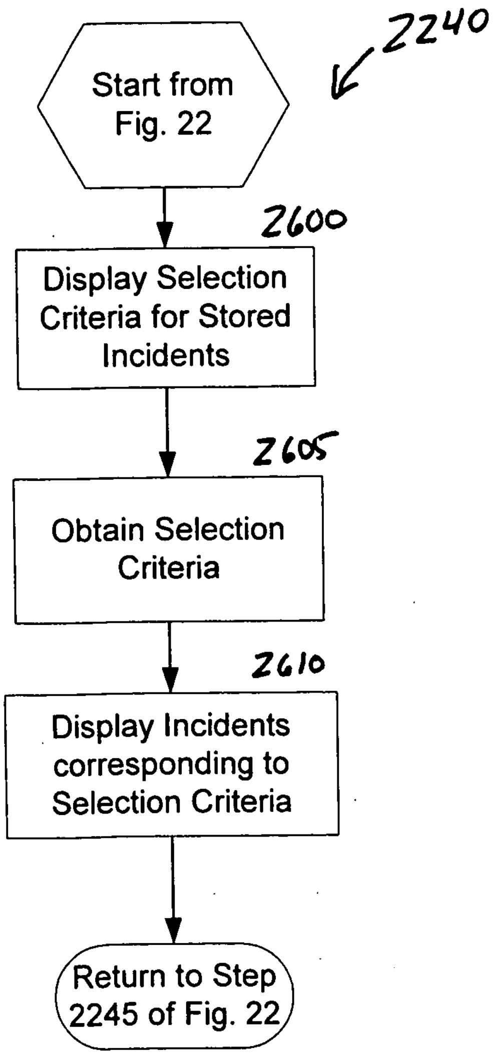

2240
Start from Fig. 22
2600
Display Selection Criteria for Stored Incidents
2605
Obtain Selection Criteria
2610
Display Incidents corresponding to Selection Criteria
Return to Step 2245 of Fig. 22

FIG. 26

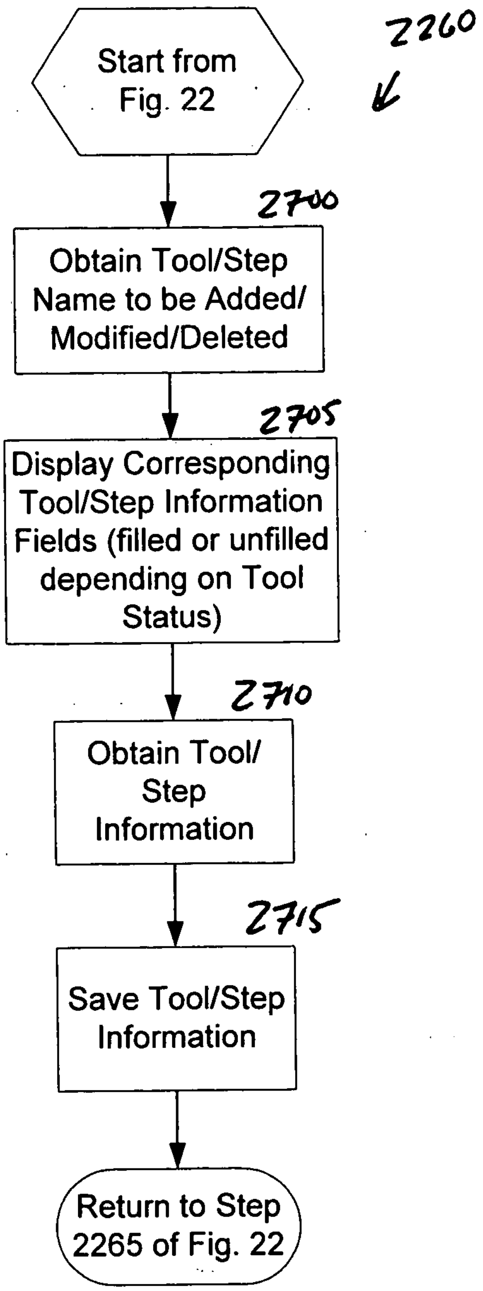

2260
Start from Fig. 22
2700
Obtain Tool/Step Name to be Added/ Modified/Deleted
2705
Display Corresponding Tool/Step Information Fields (filled or unfilled depending on Tool Status)
2710
Obtain Tool/ Step Information
2715
Save Tool/Step Information
Return to Step 2265 of Fig. 22

FIG. 27

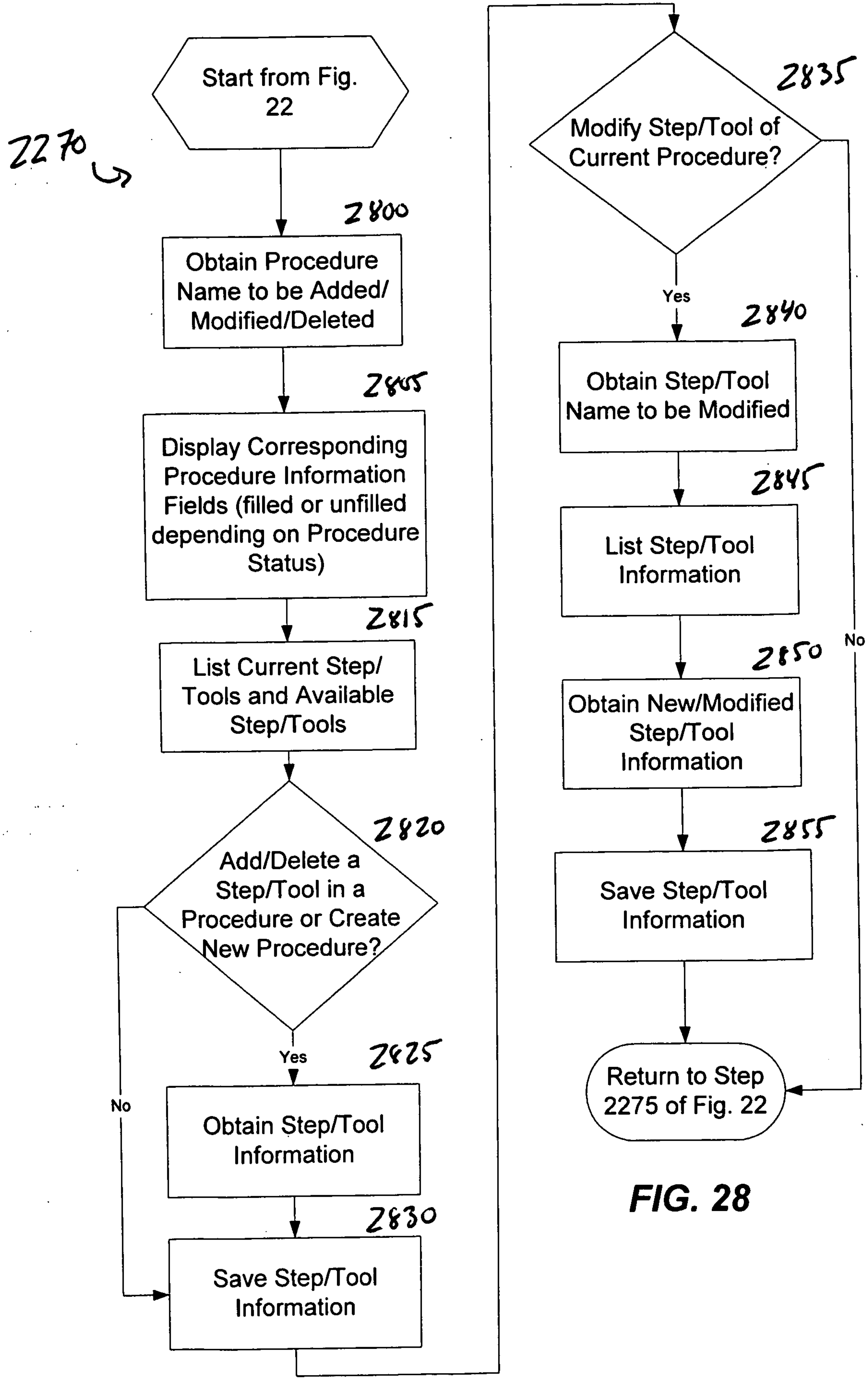

2270
Start from Fig. 22
2800
Obtain Procedure Name to be Added/ Modified/Deleted
2805
Display Corresponding Procedure Information Fields (filled or unfilled depending on Procedure Status)
2815
List Current Step/ Tools and Available Step/Tools
2820
Add/Delete a Step/Tool in a Procedure or Create New Procedure?
Yes
No
2825
Obtain Step/Tool Information
2830
Save Step/Tool Information
2835
Modify Step/Tool of Current Procedure?
Yes
No
2840
Obtain Step/Tool Name to be Modified
2845
List Step/Tool Information
2850
Obtain New/Modified Step/Tool Information
2855
Save Step/Tool Information
Return to Step 2275 of Fig. 22

FIG. 28

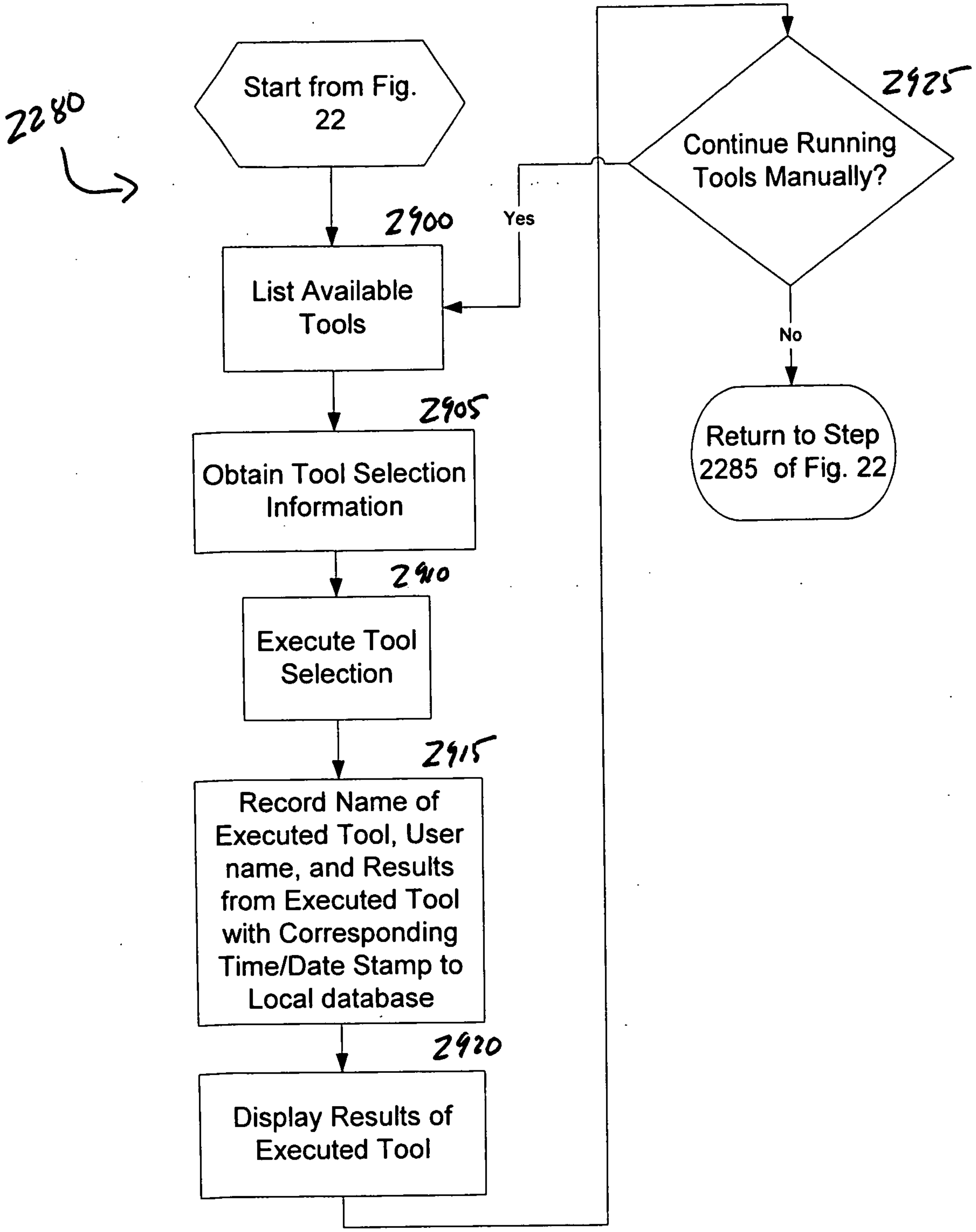

2280
Start from Fig. 22
2900
List Available Tools
2905
Obtain Tool Selection Information
2910
Execute Tool Selection
2915
Record Name of Executed Tool, User name, and Results from Executed Tool with Corresponding Time/Date Stamp to Local database
2920
Display Results of Executed Tool
2925
Continue Running Tools Manually?
Yes
No
Return to Step 2285 of Fig. 22

FIG. 29